GENERAL DATA PROTECTION REGULATION (GDPR)

Background

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018.

Definitions

The following definitions are used in this Privacy Policy:

Data Protection Legislation means all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018 or any successor legislation, and any other directly applicable European Union regulation relating to data protection and privacy; and

Personal data means information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier.

The Arts Society means the National Association of Decorative and Fine Arts Societies (operating as 'The Arts Society'), NADFAS Enterprises Limited (operating as "The Arts Society Enterprises"), and NADFAS Tours Limited (operating as "The Arts Society Tours").

Introduction

1. The Arts Society needs to process and retain certain information about its employees, trustees, volunteers, members, subscribers, grant recipients, lecturers and other members of the public to enable it to provide services and demonstrate public benefit. It is also necessary to process information so that staff can be recruited and paid, performance monitored, activities organised and legal obligations to government fulfilled.

2. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, The Arts Society must comply with the Principles which are set out in the Data Protection Legislation. In summary these state that personal data must be:
    a. obtained and processed fairly and lawfully;
    b. obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose;
    c. adequate, relevant and not excessive for that purpose;
    d. accurate and kept up to date;
    e. not be kept for longer than is necessary;
    f. processed in accordance with the data subject's rights;
    g. kept safe from unauthorised access, accidental loss or destruction;
    h. not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

3. All staff and volunteers who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens The Arts Society has adopted this Privacy Policy.

4. Any individual, who considers that this policy has not been followed in respect of personal data about him/herself, should raise the matter with the designated Data Controller initially (see 7. below). If the matter is not resolved it should be escalated to the Information Commissioner Officer (ICO).

Notification of Data Held and Processed

5. All employees, trustees, volunteers, members, subscribers, commercial partners, lecturers, and other members of the public have the right to:

- know what information The Arts Society holds and processes about them and why;
- know how to gain access to it;
- know how to keep it up to date;

- know what The Arts Society is doing to comply with its obligations under the legislation.

The Data Controller

6. The data controller determines the purposes for which and the manner in which personal data is processed. It can do this either on its own or jointly or in common with other organisations. This means that the data controller exercises overall control over the 'why' and the 'how' of a data processing activity.
7. Responsibility for this rests with the Chief Executive and the Company Secretary.

Information Held

8. Personal information is defined as any details relating to a living, identifiable individual. Within The Arts Society this applies to employees, trustees, volunteers, members, commercial partners, lecturers, and other members of the public such as job applicants and visitors.

9. Personal information is kept in order to enable The Arts Society to understand the history and activities of individuals or organisations within the voluntary and community sector and to effectively deliver services to its members and to the public. The information held may include an individual's name, postal, e-mail and other addresses, telephone numbers, bank details, subscription details, organisational roles and membership status. We need to ensure that information relating to all these people is treated correctly and with the appropriate degree of confidentiality.

10. Some personal information is defined as sensitive data and needs to be handled with special care. Sensitive data is defined by the legislation as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or a third party. At present, The Arts Society does not hold sensitive data.

Processing of Personal Information

11. All staff and volunteers who process or use any personal information are responsible for ensuring that:

- any personal information which they hold is kept securely; and
- personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

12. Staff and volunteers should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

13. Personal information should be:

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- maintained only on authorised electronic storage media which is kept securely.

Telephone Conversations and Meetings

14. If personal information is collected by telephone, callers should be advised what that information will be used for and what their rights are according to the legislation.

15. Personal or confidential information should preferably not be discussed in public areas of The Arts Society work premises or within open-plan office areas. Wherever possible, visitors should be escorted to a private room or office and not be permitted to wander about the premises on their own. If possible, visitors should subsequently be escorted out of the premises when the meeting is over. All staff should be aware of the difficulties of ensuring confidentiality in an open plan area and respect the confidential nature of any information inadvertently overheard. Any notes taken during or after an interview should be of relevance and appropriate. Such notes will be subsequently filed in a legible and coherent manner and that informal notes are retained for a short period (1 year), in a secure place, before being shredded.

Collecting Information

16. Whenever information is collected about people, they should be informed why the information is being collected, who will be able to access it and to what purposes it will be put. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of The Arts Society.

Use of The Arts Society Information

17. Information about staff, trustees and members will be used in the following circumstances:

- The Arts Society may obtain, hold, process, use and disclose information in connection with its administration, management and business activities, including making and keeping lists of members and other relevant organisations.
- The Arts Society may use information about The Arts Society and its members including lists of members, by means of newsletters or other publications.
- The Arts Society may confirm to any third party whether or not any person is a member of The Arts Society.
- The Arts Society may provide approved organisations with lists of names and contact details of members or other relevant organisations only where this is covered by one of the six lawful reasons within the legislation.
- The Arts Society may use information for anything ancillary or incidental to any of the foregoing.
- Names of, and a means of contacting, staff and trustees will be published within publicity leaflets and on the website.
- Photographs of key staff may be displayed on the website with their consent.
- The Arts Society internal staff contact list will not be a public document and information such as personal telephone numbers or home contact details will not be given out, unless prior agreement has been secured with the staff member in question.
- The Arts Society may share with you marketing information from our carefully selected affiliate partners, and other commercial organisations who support our work.
- Our current affiliate partners are:
    - Hebridean Island Cruises
    - Saga Travel
    - Fred. Olsen Cruise Lines
    - Travel Editions
    - Staysure

Confidential Material

18. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Controller.

Disposal of Confidential Material

19. Confidential material should be securely shredded. Particular care should be taken to delete information from computer hard drives if a machine is to be disposed of or passed on to another member of staff.

Staff Responsibilities

20. All staff members are responsible for checking that any information that they provide to The Arts Society in connection with their employment is accurate and up to date.

Members of staff have the right to access any personal data that is being kept about them either on computer or in manual filing systems.

21. Staff should be aware of and follow this policy and seek further guidance where necessary.

Duty to Disclose Information

22. There is a legal duty to disclose certain information, namely information about:
    - Child abuse, which will be disclosed to social services; or
    - Drug trafficking, money laundering or acts of terrorism or treason, which will be disclosed to the police.

Retention of Data

23. The Arts Society will keep some forms of information for longer than others. Because of storage limits, some information about advertisers and travel affiliates cannot be kept indefinitely, unless there are specific requests to do so. In general information about such individuals will be kept for a minimum of two years after they use the services, unless other bodies require The Arts Society to keep the information longer.

24. The Arts Society will also need to retain information about staff. In general, all information will be kept for six years after a member of staff has left The Arts Society. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

25. Training on the Privacy Policy will be given to all staff involved in processing information to ensure that data is processed correctly.

APPENDIX A: PRIVACY POLICY STATEMENT

Sharing information with others

 Sometimes we have to confirm or share information with other organisations. If we need to do this, we will make it clear to you on the forms you complete giving us the information.
 We will draw up an agreement with the organisation that we need to share the information with as appropriate. This is so that both sides understand why the information is being passed on, and what use can be made of it. In some cases, a third party organisation, such as a funding body, may draw up the agreement.

Information quality

 We will make sure that the information about you is accurate and up to date when we collect or use it. You can help us with this by keeping us informed of any changes to the information we hold about you

Information security

 We will keep information about you secure.
 We will protect your information against unauthorised change, damage, loss or theft.

Keeping information

 We will hold information about you only for as long as is necessary. After this, we will dispose of it securely and properly.

Openness

 We will tell you what kinds of information we hold and what we do with it.

Access and correctness

 Whenever possible, we will let you see the information we hold about you and correct it if it is wrong.

In general

 We will comply with the Data Protection Legislation on information handling and privacy.
 We will do this through the Privacy Policy.
 We will help you with any questions or problems that you may have with the Data Protection Legislation.
 If we cannot help you, we will give you advice on where to write to get the information you may need.

Our Commitment

 We will only collect information that is necessary for what we do.
 We will be fair in the way we collect information about you.
 We will tell you who we are and what we intend to do with the information about you.

 Where practicable, we will collect information directly from you.
 If we collect information about you from someone else, we will make sure you know that we have done this whenever possible.
 We will only share information with you from our trusted commercial partners where we believe it will be of interest.

Appendix B – Information for Local Societies

Background

On 25 May 2018 the new General Data Protection Regulation (GDPR) will come into operation. This is the first major review of data protection laws for 20 years and will seriously impact how many organisations communicate with their audiences.

The legislation has primarily been introduced to protect the privacy of individuals whilst harmonising legislation across the EU member states.

In reality it was intended to shine a light on some of the behaviour by commercial organisations and fundraising charities. However, the legislation will affect any organisation which processes "personal data". Personal data is defined as any information relating to an identified or identifiable natural person.

The legislation (The Data Protection Bill) is finishing its passage through parliament therefore although all indications are that there will be no changes to the detail or timescales, there still cannot be total certainty at this point.

The Information Commissioner's Office (ICO) which will oversee the legislation has made clear that after 25 May there will be a period when they are looking for organisations to demonstrate that they are "taking steps" to be compliant even if they haven't yet reached that point.

Interpretation

Unlike most legislation GDPR is "principles based" meaning that interpreting the rules to fit the special circumstances of your own organisation is vital.

There are six lawful reasons that can be used to justify the utilisation of personal data to communicate with your audience. Only one of the six is required and it can and will differ depending on the audience we are referring to.

The six are:

1. Consent – this is the one which has been seen most widely in the press. The requirement has been strengthened to mean that the individual must have clearly, specifically and unambiguously demonstrated their wishes. This means that no longer will pre-ticked boxes be allowed or an option to "opt out". In simple terms the individual will be "opted out" unless they explicitly advise (by ticking a box for example) otherwise. In addition there must also be an understanding of how the data will be used

2. Necessary for performance of a contract – this is where there is a situation where a transaction has occurred, and in order to satisfy the contractual relationship that now exists the communication would be required.

3. Necessary for compliance with a legal obligation – an example of this would be the retention of financial documentation for 6 years.

4. There is a “legitimate interest” – this would refer to the interest to sell something or raise money for a cause. The key questions to ask ourselves is; would the individual reasonably expect to hear from us? and would there be any negative impact on the individual through our communicating with them?

5. Vital Interests – essentially refers to “life and death” situations.

6. Public Interest – this refers to Public Authorities or those working within the public interest

There is also the additional criteria of “Implied consent”. Implied consent is created when a contract is created. For example if an individual pays to attend an event then it would be deemed as appropriate to notify them about upcoming events.

Communicating with our members

Communications sent to members to notify them of upcoming events or items of interest would fall within the criteria of both:

- Performance of a contract
- Legitimate interest

Members of local Societies automatically become members of The Arts Society in a non-voting capacity (as per the Articles of Association).

Performance of a contract and legitimate interest both override the need to gain specific consent around the utilisation of personal data for the purpose of communications.

Opting out of communications

The legislation gives the individual the right to opt out of communications (or certain types of communications)

A process must be in place whereby individuals can be removed from any mailing list immediately if they request to do so.

The right to be forgotten

The legislation introduces the “right to be forgotten”. This gives the individual the right to request that not only are they removed from any listings but any historic information is also deleted. Caution is required as this request cannot be used to override the legal requirement to hold information. The example of this being that anything relating to financial or contractual matters must be kept for 6 years. This legal basis would take precedence over the request of the individual.

Subject access requests

Individuals are able to ask what personal data is being held relating to them and for what purpose. In the event that this is requested then the request must be responded to within one month.

Retention of Data

The legislation does not stipulate how long data should be retained for. However, on inspection you must be able to explain and justify why you have chosen a specific timeframe. As a general principle 6 years is a very good starting point as this is the length of time for which data would be required in the event of needing to comply with either a financial investigation, or a breach of contract case.

Data Security and Data Access

Any personal information must be kept securely and only accessed by those who have a legitimate reason to do so.

A common sense and proportionate approach around data security and access will need to be followed depending on internal governance and operational structures. In terms of data security if information is kept in a hard copy / paper form this should be kept as securely as possible. Electronic data should be either on a password protected computer or as a password protected document.

The access to data should be at the very least restricted to a Committee and further drilled down within this to those responsible for specific communications. In some cases this would be the Programme Secretary (for the purpose of notification of events) and Treasurer (for the purposes of subscriptions and charges).

Outsourcing of processes

In the event that personal data is transferred to a third party for processing then we will have a responsibility to ensure that the third party is GDPR compliant. As part of any agreement a statement from the third party should be included confirming that they are complying with the GDPR regulations.

Demonstration of Compliance

The Information Commissioner's Office will only investigate an organisation if a complaint has been received. In the event of an investigation because of the wide scope for interpretation in the legislation, rather than looking at strict compliance, they will be focussing on reviewing the overall plan that is in place and the processes that have been implemented.

Data Breach

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorised to do so.

In the event that this occurs, the organisation has 72 hours to inform the Information Commissioner's Office unless it is unlikely to result in a risk to the rights and freedoms of the individual.

Next Steps

The key principles underpinning the legislation is the requirement for the processing of personal data to be:

- Lawful
- Fair
- Transparent

Although we have interpreted the legislation and feel that our communications fall under the joint umbrellas of contract fulfilment and legitimate interest, in the aid of transparency we feel that we need to be able to clearly answer two specific questions:

1. Why do you want my data?
2. What are you going to be doing with my data?

As part of the membership joining / renewal process we feel it would be good practice to include a narrative on the form.

A draft narrative for inclusion on the form should state:

- ***Members' details will be processed fairly and lawfully in order to satisfy the agreement entered with you on your admittance to membership. This will ensure that you receive the latest news and information about all upcoming events.***
- ***Members' details will be passed to "The Arts Society" to enable inclusion on the mailing of the quarterly magazine and other communications including information about any upcoming national events or items of legitimate interest***
- ***Members' details may be passed to "The Arts Society Area", or other affiliated societies for the purposes of disseminating relevant information of legitimate interest***
- ***Your details will be kept safely and securely and you have the ability to opt out of our communications at any time***

In Summary

We have interpreted that the processing of personal data by Societies is legal on the basis of performance of the contract entered into when the individual joined the Society.

Additionally the legal basis of "legitimate interest" is appropriate as we can be confident that a member would expect their information to be used for the purposes of disseminating information to them in accordance with their membership of the Society, and there is no reason to think that the communication of this information would negatively affect the member in any way.

Therefore consent is not required but as a matter of good housekeeping we would suggest that this is confirmed at the time of joining / renewing. It would also be good for transparency purposes to confirm how they would like to receive communications.

GDPR is a very complex area but is not designed to adversely affect the relationships which exist between the Societies and their Members. In terms of data security a common sense approach is requested. As long as we are able to satisfy ourselves that we acted in the most appropriate and proportionate way then the ICO would accept the procedures.

Once the legislation has been formally adopted we will provide a further update to confirm if there have been any material changes which would affect our interpretation.

Below is a link to the ICO website which does contain some useful additional resources.

https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/guidance-what-to-expect-and-when/

GDPR FAQ's

Do you have to delete your existing mailing lists and start from scratch? – NO

Do you need to contact everyone on the lists before 25th May 2018 and request their consent to be contacted? – NO.

After 25th May 2018 do I really have to go back on a regular basis and ask the individual again if they are happy for me to continue processing their information – YES (but this could be by way of the affirmative action of renewing their membership)

Do I really have to give them the option of withdrawing consent at any time – YES

How long should I retain data? – This needs to be looked at on a case by case basis and is a decision which must be taken by each "data holder". The key is that you must be able to justify how long you are holding data. Financial information must legally be retained for 6 years.

I must keep data secure. What does this mean? – This must be proportionate and common sense should be applied. Where there is a risk that the data can be accessed by anyone other than the intended recipient then additional steps (locked cabinets / password protection) should be taken.

Tim Nicholls
Finance and Resources Director
Aug 2021