

ABPS

General Data Protection Regulations (GDPR)

Good Practice Guidelines

These good practice guidelines are aimed at local philatelic societies and federations and refer to the GDPR that are in force from the 25 May 2018.

Note: The ABPS is not responsible for ensuring that societies and federations follow these guidelines.

1. What are the principles to be adhered to in order to comply with the GDPR.
 - Lawfulness, fairness and transparency
 - "Purpose" limitation must be specified, explicit and legitimate.
 - Data minimization – only hold data that is needed.
 - Accuracy (put in place systems to ensure that data is accurate).
 - Storage limitations – hold data only for as long as it is needed.
 - Data Security – ensure data is held securely, whether it is on paper or electronically.
 - Data Subjects Rights (refer to paragraph 2)
 - Accountability (refer to paragraph 6).

2. Data Subject Rights

Jargon: Data Subject is the person who has provided the personal data.

- Right of Access
- Right to rectify
- Right to erasure
- Right not to be subject to automated decision making (in reality this right is unlikely to affect local societies or Federations).

Note: Any request to use these rights must be dealt with within one month of notification.

3. Consent

- Consent is only one of the grounds to allow for lawful processing of personal data. The other grounds are for the allowing of a performance of a contract and the other is to comply with a legal obligation these are unlikely to be encountered by a Society.
- Consent must be obtained to use the supplied data and only for **specified, explicit** and legitimate reasons.
- Consent must be obtained through the use of a tick box or signature or other active consent method.

Note: The need for consent only applies when using the personal data in a public forum or passing information to third parties. If a local Society only uses the data for internal purposes there is no requirement to obtain consent. However be careful if you do this that there is no personal data (you can include names) in newsletters or websites ensure that contact details are generic such as secretary@philatelicsociety.org.

4. Data minimization

- Decide what information you require and why you need it. Do not collect data because one day it might be useful, this is not allowed.
- It is suggested that the minimum information required to run an efficient society will be:
 - Name
 - Address
 - Telephone
 - Email address
 - Social media (if applicable)

Note: the recording of an address would be reasonable in order to send out notices, for running an exchange packet and for those without email.

TIP: be very careful recording data in the class defined as "Special Personal Data" e.g. religion, ethnicity, health, sexual orientation + others as they have other regulations applied to them.

5. Accuracy

- Put in place some system to ensure as far as possible that the data held is accurate. In reality this could be a check on renewal of subscriptions that all members are asked to confirm that their personal data is up to date.

6. Storage limitations

- Under the GDPR there is no stipulated period of time that data can be held. However data should only be held for the period that it is required. It would be reasonable that after initial consent is given and a subscription to a Society is paid (or membership rights given) that on renewal of that subscription (or membership rights extended) that a continuation of that consent along with the other obligations such as adherence to the Society's Constitution is in place.
- Once a Society member resigns or does not renew their subscription the reason for keeping their data has been removed and it would be reasonable to delete it at the end of the following subscription period.

7. Accountability

- Societies and Federations should have a written policy in place outlining their method of handling their data, for what purpose they are going to use that data, who is responsible for holding, processing that data and answering any rights issues notified to the Society.

TIP: This need only be a short statement in a committee meeting minutes stating that it will be used for the purpose of the efficient running of the society (and any exchange packet) and naming the person in charge of the data.

TIP: Do not appoint a "Data Processing Officer" as defined under the GDPR, this is not required and bestows onerous duties under the act.

Jargon: The GDPR uses two names "Data Controller" is someone who owns the data and "Data Processor" is someone who processes that data e.g. sending out newsletters, exchange packets, etc. For a Society they can be regarded as being the same (unless a third party is used).

Note: For Societies that use third party printing and mailing firms for Journals, etc. a data sharing agreement should be used. This is not onerous as all printing firms are familiar with these and will have them in place.

8. Checklist

- Appoint a person to be responsible for the secure holding of the data and responsible for answering any Data Subject Rights.
 - **TIP:** usually this would be the membership secretary.
- Ensure that all other members of the Society are aware of this appointment and that they are not allowed to hand out to third parties member contact details without consent.
- The society management committee to stipulate when and why personal data can be used and record it in the minutes.
- Empower the person handling the data to gain consent from all existing members and each new member (refer to Appendix A).
- Review the consent form and if any major changes are required gain renewed consent from all members.

APPENDIX A – suggested consent template:

"Data handling agreement

Purpose - Somewhere & District Stamp Club will use and hold the supplied data for the purpose of organising the Club, running the exchange packet, promoting philately in the local Federation area and to provide services to the membership.

Period of holding the data – Somewhere & District Stamp Club will hold the data until instructed otherwise.

Cancellation - you can cancel this agreement at anytime and your details will be removed. Please contact the Somewhere & District Stamp Club Secretary.

Security of data - Somewhere & District Stamp Club will handle the data in a secure form and will not distribute to third parties other than for the purpose outlined above.

Agreement - I understand that the data provided will be used for the outlined purpose.

Signed _____ Date _____

Print name _____"

ABPS General Secretary

General Data Protection Regulations v1
January 2018