Easter Orchestal Society (EOS) Data Protection policy

Overview

Key details

- Policy prepared by the EOS Committee
- Approved by the EOS Committee on: May 2018
- Next review date: May 2020

Introduction

To operate, the Easter Orchestral Society (EOS) needs to gather, store and use certain forms of information about individuals.

These can include members, employees, contractors, suppliers, volunteers, audiences and potential audiences, business contacts and other people the group has a relationship with or regularly needs to contact.

This policy explains how this data should be collected, stored and used to meet EOS data protection standards and comply with the General Data Protection Regulations (GDPR).

Why is this policy important?

This policy ensures that EOS:

- Protects the rights of our members, volunteers and supporters
- Complies with data protection law and follows good practice
- Protect the group from the risks of a data breach

Roles and responsibilities

Who and what does this policy apply to?

This applies to *all* those handling data on behalf of EOS e.g.:

- Committee members
- Employees and volunteers
- Members
- Contractors/3rd-party suppliers

It applies to all data that EOS holds relating to individuals, including:

- Names

- Email addresses
- Postal addresses
- Phone numbers
- Any other personal information held (e.g. financial)

Roles and responsibilities

EOS is the Data Controller and will determine what data is collected and how it is used. The Data Protection Officer for EOS is the Secretary. The Secretary, together with the Committee, is responsible for the secure, fair and transparent collection and use of data by EOS. Any questions relating to the collection or use of data should be directed to the Data Protection Officer.

Everyone who has access to data as part of EOS has a responsibility to ensure that they adhere to this policy.

If EOS uses third party Data Processors (e.g. [Mail Chimp]) to process data on its behalf, EOS will ensure all Data Processors are compliant with GDPR.

Data protection principles

a) We fairly and lawfully process personal data in a transparent way

EOS will only collect data where lawful and where it is necessary for the legitimate purposes of the group.

- A member's name and contact details will be collected when they first join the group, and will be used to contact the member regarding group membership administration and activities. Other data may also subsequently be collected in relation to their membership, including their payment history for 'subs'.
- The name and contact details of volunteers, employees and contractors will be collected when they take up a position, and will be used to contact them regarding group administration related to their role.

  Further information, including personal financial information and criminal records information may also be collected in specific circumstances where lawful and necessary (in order to process payment to the person or in order to carry out a DBS check).
- An individual's name and contact details will be collected when they make a booking for an event. This will be used to contact them about their booking and to allow them entry to the event.
- An individual's name, contact details and other details may be collected at any time (including when booking tickets or at an event), with their consent, in order for EOS to communicate with them about and promote group activities. See 'How we get consent' below.
- Pseudonymous or anonymous data (including behavioural, technological and geographical/regional) on an individual may be collected via tracking 'cookies' when they access our website or interact with our emails, in order for us to monitor and improve our effectiveness on these channels. See 'Cookies on the EOS website' below.

b) We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.

When collecting data, EOS will always provide a clear and specific privacy statement explaining to the subject why the data is required and what it will be used for.

c) We ensure any data collected is relevant and not excessive

EOS will not collect or store more data than the minimum information required for its intended purpose.

E.g. we need to collect telephone numbers from members in order to be able to contact them about group administration, but data on their marital status or sexuality will not be collected, since it is unnecessary and excessive for the purposes of group administration.

d) We ensure data is accurate and up-to-date

EOS will ask members, volunteers and staff to check and update their data on an annual basis. Any individual will be able to update their data at any point by contacting the Data Protection Officer.

e) We ensure data is not kept longer than necessary

EOS will keep records for no longer than is necessary in order to meet the intended use for which it was gathered (unless there is a legal requirement to keep records).

The storage and intended use of data will be reviewed in line with EOS's data retention policy. When the intended use is no longer applicable (e.g. contact details for a member who has left the group), the data will be deleted within a reasonable period.

f) We keep personal data secure

EOS will ensure that data held by us is kept secure.

- Electronically-held data will be held within a password-protected and secure environment
- Passwords for electronic data files will be re-set each time an individual with data access leaves their role/position
- Physically-held data (e.g. membership forms or email sign-up sheets) will be stored in a locked cupboard
- Keys for locks securing physical data files should be collected by the Data Protection Officer from any individual with access if they leave their role/position. The codes on combination locks should be changed each time an individual with data access leaves their role/position
- Access to data will only be given to relevant trustees/committee members/contractors where it is clearly necessary for the running of the group. The Data Protection Officer will decide in what situations this is applicable and will keep a master list of who has access to data

g) Transfer to countries outside the EEA

EOS will not transfer data to countries outside the European Economic Area (EEA), unless the country has adequate protection for the individual's data privacy rights.

Individual Rights

When EOS collects, holds and uses an individual's personal data that individual has the following the rights over that data. EOS will ensure its data processes comply with those rights and will make all reasonable efforts to fulfil requests from an individual in relation to those rights.

Individual's rights

- *Right to be informed:* whenever EOS collects data it will provide a clear and specific privacy statement explaining why it is being collected and how it will be used.

- *Right of access:* individuals can request to see the data EOS holds on them and confirmation of how it is being used. Requests should be made in writing to the Data Protection Officer and will be complied with free of charge and within one month. Where requests are complex or numerous this may be extended to two months

- *Right to rectification:* individuals can request that their data be updated where it is inaccurate or incomplete. EOS will request that members, staff and contractors check and update their data on an annual basis. Any requests for data to be updated will be processed within one month.

- *Right to object:* individuals can object to their data being used for a particular purpose. EOS will always provide a way for an individual to withdraw consent in all marketing communications. Where we receive a request to stop using data we will comply unless we have a lawful reason to use the data for legitimate interests or contractual obligation.

- *Right to erasure:* individuals can request for all data held on them to be deleted. [Group name's] data retention policy will ensure data is not held for longer than is reasonably necessary in relation to the purpose it was originally collected. If a request for deletion is made we will comply with the request unless:
- There is a lawful reason to keep and use the data for legitimate interests or contractual obligation.

- There is a legal requirement to keep the data.

Right to restrict processing: individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if they have contested the accuracy of any of their data, EOS will restrict the data while it is verified).

Though unlikely to apply to the data processed by EOS, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

Member-to-member contact

We only share members' data with other members with the subject's prior consent

As a membership organisation EOS encourages communication between members.

To facilitate this:

- Members can request the personal contact data of other members in writing via the Data Protection Officer or Membership Secretary. These details will be given, as long as they are for the purposes of contacting the subject (e.g. an email address, not financial or health data) and the subject has consented to their data being shared with other members in this way

How we get consent

EOS will regularly collect data from consenting supporters for marketing purposes. This includes contacting them to promote performances, updating them about group news, fundraising and other group activities.

Any time data is collected for this purpose, we will provide:

- A method for users to show their positive and active consent to receive these communications (e.g. a 'tick box')
- A clear and specific explanation of what the data will be used for (e.g. 'Tick this box if you would like EOS to send you email updates with details about our forthcoming events, fundraising activities and opportunities to get involved')

Data collected will only ever be used in the way described and consented to (e.g. we will not use email data in order to market 3rd-party products unless this has been explicitly consented to).

Every marketing communication will contain a method through which a recipient can withdraw their consent (e.g. an 'unsubscribe' link in an email). Opt-out requests such as this will be processed within 14 days.

Cookies on the EOS website

A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

EOS may use cookies on our website to to improve users' experience of our website by, for example, allowing for a 'logged in' state, and by giving us useful insight into how users as a whole are engaging with the website.

When we use cookies on our website, we will implement a pop-up box on that will activate each new time a user visits the website. This will allow them to click to consent (or not) to continuing with cookies enabled, or to ignore the message and continue browsing (i.e. give their implied consent).

It will also include a link to our Privacy Policy which outlines which specific cookies are used and how cookies can be disabled in the most common browsers.

Data retention policy

Overview

Introduction

This policy sets out how EOS will approach data retention and establishes processes to ensure we do not hold data for longer than is necessary.

It forms part of EOS Data Protection Policy.

Roles and responsibilities

EOS is the Data Controller and will determine what data is collected, retained and how it is used. The Data Protection Officer for EOS is the Secretary. They, together with the Committee, are responsible for the secure and fair retention and use of data by EOS. Any questions relating to data retention or use of data should be directed to the Data Protection Officer.

Regular Data Review

A regular review of all data will take place to establish if EOS still has good reason to keep and use the data held at the time of the review.

As a general rule a data review will be held every 2 years and no more than 27 calendar months after the last review. The first review took place on 1 June 2018.

Data to be reviewed

- EOS stores data on digital documents (e.g. spreadsheets) stored on personal devices held by committee members.
- Data stored on third party online services [(e.g. Google Drive, Mail Chimp)]
- Physical data stored at the homes of committee members

Who the review will be conducted by

The review will be conducted by the Data Protection Officer with other committee members to be decided on at the time of the review.

How data will be deleted

- Physical data will be destroyed safely and securely, including shredding.
- All reasonable and practical efforts will be made to remove data stored digitally.
    - Priority will be given to any instances where data is stored in active lists (e.g. where it could be used) and to sensitive data.
    - Where deleting the data would mean deleting other data that we have a valid lawful reason to keep (e.g. on old emails) then the data may be retained safely and securely but not used.

Criteria

The following criteria will be used to make a decision about what data to keep and what to delete.

Question	**Action**	
	Yes	**No**
Is the data stored securely?	No action necessary	Update storage protocol in line with Data Protection policy
Does the original reason for having the data still apply?	Continue to use	Delete or remove data
Is the data being used for its original intention?	Continue to use	Either delete/remove or record lawful basis for use and get consent if necessary
Is there a statutory requirement to keep the data?	Keep the data at least until the statutory minimum no longer applies	Delete or remove the data unless we have reason to keep the data under other criteria.
Is the data accurate?	Continue to use	Ask the subject to confirm/update details
Where appropriate do we have consent to use the data. This consent could be implied by previous use and engagement by the individual	Continue to use	Get consent
Can the data be anonymised	Anonymise data	Continue to use

Statutory Requirements

Date stored by EOS may be retained based in statutory requirements for storing data other than data protection regulations. This might include but is not limited to:

- Gift Aid declarations records
- Details of payments made and received (e.g. in bank statements and accounting records)
- Trustee meeting minutes
- Contracts and agreements with suppliers/customers
- Insurance details
- Tax and employment records

Other data retention procedures

Member data

- When a member leaves EOS and all administrative tasks relating to their membership have been completed any potentially sensitive data held on them will be deleted – this might include bank details or medical data
- Unless consent has been given data will be removed from all email mailing lists
- All other data will be stored safely and securely and reviewed as part of the next two year review

Mailing list data

- If an individual opts out of a mailing list their data will be removed as soon as is practically possible.
- All other data will be stored safely and securely and reviewed as part of the next two year review

Volunteer and freelancer data

- When a volunteer or freelancer stops working with EOS and all administrative tasks relating to their work have been completed any potentially sensitive data held on them will be deleted – this might include bank details or medical data
- Unless consent has been given data will be removed from all email mailing lists
- All other data will be stored safely and securely and reviewed as part of the next two year review

Other data

- All other data will be included in a regular two year review.