General Data Protection Regulations (GDPR) - 2018
Policy

Introduction

The GDPR came into effect in May 2018 and is an evolution of older data privacy law. Although it demands more from Societies than the pre-2018 regime in terms of accountability, compliance should be common sense, and a matter of building on existing foundations.

In the UK, the Information Commissioner's Office (ICO) is responsible for regulating data privacy. In addition to the power to impose administrative fines, they also have a number of investigative, corrective and advisory powers.

The aim of the GDPR is to ensure good information handling practice and is essentially about trust and responsibility. Organisations and Societies have become accountable for their use of "personal data", and must be able to demonstrate that they process and handle "personal data" in a fair, lawful and responsible manner.

Methodology

Reference to NODA's (National Operatic and Dramatic Association) 'An introduction to GDPR' has been used in the production of this policy.

Scope

This policy applies to RATS members & supports, Youth Theatre (YT) members and their parents/guardians), and patrons on RATS mailing list.

Personal data

Personal data is defined broadly and comprises data relating to any living individual who can be identified from that data. From RATS perspective this is the data (such as names, addresses, email addresses, telephone numbers, dates of birth, photographs, videos and the like) that is held about members, supporters, YT members, patrons and those who attend productions and events (where data is collected from ticket sales), and anyone who makes a donation.

In essence the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects (the individual to whom personal data relates) for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security.

Reasons for using Personal Data

RATS must have a lawful reason (or basis) for the use of someone's personal data. They are:

- consent
- contract
- legal obligation
- vital interests
- public task and
- legitimate interests

Deciding on which lawful basis applies will depend on the specific purposes and the context of the processing. In many cases, the choice is between using '*legitimate interests'* or '*consent*'.

**Legitimate interests* – are likely to be most appropriate where the use of an individual's data would be reasonably expected, and which has a minimal privacy impact.
**Consent* – gives individuals full control and responsibility for their data.

Organisations and Societies must determine the lawful basis before processing personal data and communicate this information in their Privacy Policy. Individuals need to be given (amongst other things) the intended purposes for processing and the lawful basis being relied upon.

The GDPR introduced new rights including the right to erase personal data (aka the "**right to be forgotten*"), to restrict data processing under certain circumstances, and data portability.
Appendix 1 – *further information

RATS Governance arrangements

RATS Committee will act as:

The Data Controller: an individual or body which, alone or jointly with others, determines the purpose and means of the processing of personal data. They are also responsible for and must be able to demonstrate compliance with the GDPR.
The Data Processor: an individual or body which processes personal data on behalf of the controller.

RATS Committee will be responsible for:

Processing: any operation which is performed on personal data, whether or not by automated means, such a collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosue by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Filing systems: any structural set of personal data (paper or electronic) which makes personal data accessible according to specific criteria.
Appointing a Data Representative: a designated Committee member
Ensuring: RATS Privacy Policy accords with the GDPR
Assessing and recording the likely data protection impact of:

- personal data collected and stored
- any new data processing activity

Failure to get data privacy right is likely to damage RATS reputation, its audiences, relationships, and ultimately, finances.

Duties to report a breach

RATS Committee has a duty to report a breach of the GDPR and will notify the ICO within 72 hours of the discovery of any breach where it is likely to result in a risk to the rights and freedoms of individuals. Assessing the risk will be considered on a case-by-case basis, but the following factors should be taken into account:

- the type of breach (such as the loss of confidential information)
- the nature, sensitivity and volume of personal data lost
- the ease of identification of individuals
- the severity of consequences for individuals
- any special characteristics of the individual (for example whether they are children or another class of vulnerable individuals)
- the number of affected individuals

When reporting a breach RATS will provide:

- a description of the nature of the personal data breach
- contact details for the RATS Data Representative
- a description of the likely consequences of the personal data breach
- a description of the measures taken / proposed to be taken to deal with the personal data breach and (where appropriate) mitigate any possible adverse effects

Data Representative – Julie Hesketh, Secretary (First point of contact)

Appendix 1 Further information – *Legitimate Interest / Consent / Right to be Forgotten*

Legitimate interests

There are three elements to the *legitimate interests* basis. You need to:

1. identify a legitimate interest (e.g. promoting a Society's production)
2. be clear that the processing is necessary to achieve it (e.g. you have to send information and/or invitations to individuals to promote the production), and
3. balance it against the individual's interests, rights and freedoms (e.g. a Society's interest in promoting a production outweighs the members'/previous attendees' right not to be contacted)

Consent

Consent now must be unambiguous, freely given, involve a positive action, be clearly separate from other terms.

The individual must be made aware of the identity of the Data Controller, the purpose of the processing and the types of processing activity.

Organisations and Societies must make it easy for people to exercise their right to withdraw *consent*. Furthermore, wherever consent has been relied upon in the past, they should review the information to ensure that they continue to meet the standard. If not, then they will require updating.

The Right to be Forgotten

The right to erase personal data, to restrict processing under certain circumstances, and data portability.

Other rights under the GDPR include the right to correct personal data, object to processing, and the right not to be subject to automated decision-making. The rights conferred by the GDPR are subject in each case to certain qualifications. For instance, Data Controllers must delete personal data on request where specified grounds apply. Those grounds include where the personal data is no longer necessary for the original purpose for which the data was collected/processed and if the data subject withdraws their consent, and no other legal ground for processing applies. However, there are a number of grounds on which Data Controllers can rely to keep personal data. These include compelling legitimate grounds, compliance with a legal obligation, or the establishment, exercise or defense of legal claims.

Personal data should not be kept for longer than needed and safe and secure storage of that data is paramount when it is kept.