GDPR Briefing

General Committee 5th March 2018

What is it?

The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018.

GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR brings in a much broader definition of personal data from previous legislation, increases the standard of consent needed and the obligations to protect and secure information under our control.

GDPR retains the existing rights of data subjects and introduces enhanced rights including the right of 'erasure' (to be forgotten, although there can be compelling reasons to continue processing data), data portability and extended rights to object and be informed. Consent will become a restricted concept under the GDPR in that it must be freely given, specific, informed and an unambiguous indication of the data subject's wishes.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Our Current Situation

The Surrey Association uses very little personal data. The majority of our members and tower contacts are known by name only together with their associated tower and in many cases an email address. For newer members we store address and phone number information where provided at the time of joining. We don't hold age, date of birth or any sensitive data except for some minors (see below).

One important feature of our current systems is information is distributed across a number of different officers who perform defined functions. Data is kept for the specific purpose of the individuals and not seen as a collective resource.

We hold limited information on minors, identified only by their subscription band in treasurer records. The exception to this is where a parental consent form has been provided permitting a minor to take part in an Association event. This form contains additional personal information including date of birth and medical information as well as contact details for a parent and/or emergency contact.

Systems for storing data vary, we have a mix of paper, local PC files and cloud based records. There is no consistent policy on data security or privacy with individual officers left to take their own decisions and measures.

There is no consistent approach to updating or deleting data when it is no longer needed. Data housekeeping is left to individuals and information on changes is not necessarily shared.

The majority of our data is held without any explicit consent. Limited consents are available for newer members, training course attendees and minors regarding publication of photos online. Consent however is not just about a box on a form, the systems to record, enforce and update a consent (or withdrawal of consent) are deficient and this information is not shared.

A particular concern is the publication of members names without an explicit consent to do so. This happens in the annual report and for numbers club winners.

As a voluntary association officers change frequently and data is passed on from departing to new people. There is no policy on security of transmission of data between parties or training for new officers in their data protection obligations.

There is more information about GDPR and links to third party resources on our website at:http://wiki.surreybellringers.org.uk/association/gdpr. You are recommended to familiarise yourself with this information

The association officers typically use their own email addresses for conducting association business which means the evidence and audit trail for changes exists in their personal records not the associations.

Our biggest problem is……

Our current system of membership records is based on collecting subscriptions, a process that needs minimal information and is often mediated through towers. The systems are personalised, informal and designed to deal with minimal data used for a single purpose.

Unfortunately, this means the data needs of other functions are ignored and we are starved of the data needed to properly know our members, engage with them and promote our activities.

The effect of this is we are over reliant on the Yahoo groups for contacting members and a system of cascading information through tower contacts which is widely believed to be ineffective. This vacuum of good quality and UpToDate information about our membership inhibits community growth and prosperity and is often filled with ad-hoc, home brew solutions which expose the association to risk of failures in its obligation to protect individual's data.

The association would benefit from a more coherent and centralised process of membership management which would allow us to keep richer information with consent, use it in more ways to benefit the community and make data protection controls easier to implement.

Conclusion: Continuing to operate as we do now risks falling foul of the new data protection environment and puts the long term success of the association in jeopardy.

Penalties for Data Protection Offences

Surely it's only big companies that get fined for data protection offences? Not true the UK regulator (the ICO) has prosecuted and fined numerous charities and voluntary organisations under the existing data protection legislation. These are just a few of many charities fined in 2017:

- Battersea Dogs and Cats Home (fined £9,000)
- Great Ormond Street Hospital Children's Charity (fined £11,000)
- Macmillan Cancer Support (fined £14,000)
- The Royal British Legion (fined £12,000)

GDPR increases the level of fines the ICO can levy, raises the standards that organisations need to adhere to and gives individuals more rights to ensure their data is protected.

GDPR - What do we have to do?

There are many different provisions in the GDPR but most relevant for us are the following three areas:

1. Establish a lawful basis for the data we process (article 6). Two options are available, we can claim a 'legitimate interest' or seek an explicit 'consent'. Both options come with constraints and obligations.

2. Be transparent about what data we have and how we use it and provide information about how we protect individual's rights (article 12).

3. Implement appropriate technical and organisational measures to show that we have considered and integrated data protection into our processing activities (article 25).

Each of these is described in more detail below.

There is more information about GDPR and links to third party resources on our website at:http://wiki.surreybellringers.org.uk/association/gdpr. You are recommended to familiarise yourself with this information

Lawful Basis

Legitimate interest - If we use the minimum necessary data for purposes that someone would reasonably expect us to use it for (i.e. membership records) we can operate under a 'legitimate interest' provided we do nothing to override the individual rights or freedoms.

Legitimate interest provides a legal basis for maintaining membership records but does not cover activities such as publishing personal information in our annual report, newsletter or website which could potentially infringe a person's right to privacy.

Consent - We can seek individuals consent to carry out specific defined processing but this comes with an increased burden in collecting, maintaining and adhering to those consents.

GDPR defines consent as a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. Additional conditions apply when consent is required from a minor.

None of the data we hold now has sufficient consent for us to continue using it on this basis and our operating procedures are insufficient to maintain and apply any consents we collect.

Transparency

GDPR sets down clear guidelines on what information we need to publish and how it should be communicated.

Information provided to individuals should be; concise, transparent, intelligible and easily accessible; andwritten in clear and plain language, particularly if addressed to a child;

Information we are required by law to provide includes:

- The lawful basis for our data processing,
- What data we hold, why we need it and how it is used,
- How long we keep the data for,
- Information about an individual's rights and how to complain.

Making data protection inherent to the way we work

Under the GDPR (Article 25), we have a general obligation to implement appropriate technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

Our systems need to ensure that we:

- only keep personal data which is absolutely necessary for the purpose.
- delete data that is no longer required.
- secure data and ensure it is only accessible to those authorised to use it.
- privacy is the default setting and we do not share data without the explicit consent of the individual.

We need to review our existing practices and if necessary implement changes to ensure data is properly protected and controlled.

There is more information about GDPR and links to third party resources on our website at:http://wiki.surreybellringers.org.uk/association/gdpr. You are recommended to familiarise yourself with this information

Draft Action Plan

This action plan focusses on practical changes the association can make in the short term to respond to the changing regulatory environment and reduce risk whilst a review is undertaken into how to achieve full compliance.

Step 1:

1- Understand the legislation and the impact it has on us.
2- Conduct a review of what data we hold
3- Ensure the officers and members are informed about the new regulation.
4- Provoke meaningful debate about the way the association is impacted by these regulations and how we respond

Rationale: These steps are recommended best practice and demonstrate that the organisation is taking the new regulation seriously.

Step 2:

1- Limit our activities to what we can claim as 'Legitimate Interest' only and stop doing anything that may require consent until we can implement appropriate processes for collecting and managing that consent.

Specifically this means:

- Stop publishing members names and contact details in the Annual Report.
- Seek consent from all numbers club members to ensure we can identify them as a member and publish their names when they win prizes. This could be done as a rolling process as members renew their annual subscription. Ensure we can effectively handle 'anonymous' members.
- Rationalise tower contact information and produce a master list of approved tower contacts.
- Review data protection and consent provided for training events and training days.

2- Extend our privacy policy to cover all of our current data processing and make this available to all members.

3- Make sure association officers are adequately trained in data protection.

4- Define standards and best practices for data security and privacy for association officers to follow when processing data on behalf of the association and have them 'self certify' to these.

Rationale: These steps are all prudent and include recommended best practice. They can all be implemented fairly easily at little or no cost.

Step 3:

Review our operating model and make recommendations for changes to systems and processes so that we can fully comply with data protection regulations and make better use of the data we have.

Rationale: The association would benefit from a more coherent and centralised process of membership management which would allow us to keep richer information with consent, use it in more ways to benefit the community and make data protection controls easier to implement.

There is more information about GDPR and links to third party resources on our website at:http://wiki.surreybellringers.org.uk/association/gdpr. You are recommended to familiarise yourself with this information