The General Data Protection Regulations (GDPR)

Introduction

Any group, club or branch which brings people together to dance is likely to end up handling personal information. In most cases, this will be names and contact details, such as an address, telephone number or email address. However, personal information can also include a person's age, date of birth, nationality and details of any special requirements that they may have. You may hold this type of information for dancers, members, volunteers, teachers and/or those attending events.

Many countries have their own data protection laws, which are likely to have been in place for some time. However, the law that applies to all EU countries is changing on 25th May 2018 with the introduction of the General Data Protection Regulations (more commonly known as 'GDPR'). These changes will take effect where personal information is processed within the European Economic Area (EEA) regardless of whether the subject of the information ("data subject") is an EU or EEA citizen or not, or whether they live in the EEA or not (i.e. it is where the processing of information takes place that matters). Please note that data protection laws, including GDPR, apply to personal information about living individuals and not to information about organisations.

GDPR is an evolution of existing data protection law so, while there are some important new elements, such as those outlined in this guidance, it does ***not*** mean a complete overhaul of systems and procedures.

This guidance is designed to provide a summary of the main relevant points around GDPR for all RSCDS branches and Affiliate Groups. It does not therefore contain a full list of everything that you may need to do to satisfy the law. We strongly recommend all groups and branches make themselves familiar with additional guidance, such as that that produced by the UK's Information Commissioners Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

Who does GDPR apply to?

The RSCDS has spent time in discussion with the UK's Information Commissioner's Office to clarify how and to whom it should and shouldn't apply. To be clear:

- *GDPR will apply to the day-to-day operation of branches, affiliate groups and other clubs who operate within the European Economic Area (EEA)[1].*

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom

- *GDPR will **not** apply to the day-to-day operation of branches, affiliate groups and other clubs, who operate outside the EEA. This is the case even where those branches, affiliate groups and clubs hold personal information for EEA nationals.*
- *Although GDPR will not apply to the day-to-day operation of RSCDS branches outside the EEA, those branches will still be processing membership information which is covered by GDPR (because they will share information with RSCDS which is based in the EEA) . A contractual 'data transfer agreement' will therefore need to be in place between RSCDS and these branches, to ensure that both parties are contractually compliant with GDPR.*

General points on GDPR

There are a few components of GDPR, which you should familiarise yourself with and, potentially, take action on.

1. Consent / Lawful Bases for Processing

You must have a valid lawful basis for processing personal information. There are a number of lawful bases for processing, which are set out in detail here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/. However, the vast majority of personal information that is likely to be handled by branches and groups will be handled under one of the following legal bases:

a) *Legitimate Interest* – this applies where you have a clear and identifiable legitimate interest for using people's information. Relevant examples here may be when administering club membership or for managing event bookings.

   The UK's Information Commissioners Office recommends undertaking a quick test to satisfy yourself that you can use this basis, with details here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. You should record any assessment you undertake under this basis.

b) *Vital Interests* – where you need to process information to protect someone. An example here would be if you report a safeguarding concern.

c) *Legal Obligation* – where you are processing information to fulfil a legal obligation. Examples here would include sending tax information to authorities or when requested to do so as part of a criminal investigation

d) *Contractual Obligation* – where you are processing information to fulfil a contractual obligation to the data subject (for example if they are purchasing something from you or if you employ them) or because they have asked you to do something before entering into a contract (e.g. when someone has applied for a job/position in your organisation).

The final lawful basis that is often mentioned when using personal information is consent. This should be used only when there is not another clear lawful basis which covers the processing, such as when undertaking marketing or fundraising activity. In cases like this consent must be gained through a positive 'opt-in' by the data subject.

Further information on consent is available from the UK's Information Commissioners Office here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/.

The requirement for consent has caused a lot of confusion, with many people under the impression that consent is required for every use of personal data. The reality is that in many cases it will not be required. To use RSCDS as an example:

We do not need to seek positive opt-in consent from members for processing any element of their membership, such as discount on shop orders or distribution of the Scottish Country Dancer magazine. That is because we regard this activity as a 'Legitimate Interest' in processing the membership that they have with us.

However, if we decided to distribute new marketing messages (e.g around fundraising), this activity would not be regarded as a justifiable legitimate interest and we would usually need to seek positive opt-in consent.

It should be noted that consent must be "freely given, specific, informed and unambiguous". In general, this will mean you cannot use consent to process personal information for anyone over whom you have authority/influence such as an employee (who will rely on you for their income).

2. Data Protection Principles

While data protection law may vary from country to country, there are a number of existing principles which organisations will be required to continue to abide by for GDPR. They require that personal information is:

a) *Processed lawfully, fairly and transparently*. This means that you must not do anything unlawful with personal information and only use it for purposes that those people expect.

b) Obtained only for one or more specific and lawful purpose. This means you must be clear about why you are collecting the information and what you plan to do with it. A simple way to do this is to provide a short privacy notice when collecting information (sample privacy notices can be found at the end of this guidance).

c) Adequate and relevant to the purpose for which it will be used. This means that you should only hold the information that you need, for the purposes that you identified, and nothing more. An example would be holding information on educational qualifications or nationality, neither of which is likely to be relevant.

d) *Accurate and, where necessary, kept up to date.* This principle is very straightforward, requiring organisations to ensure that they update information, where someone has flagged up that it is incorrect.

e) *Kept for no longer than is necessary for that purpose.* There is no minimum or maximum period for which you are allowed to hold personal information. This principle therefore simply requires that you only keep information for as long as it is needed, reviewing what you hold and securely deleting information that is no longer needed.

f) *Processed in a manner that ensures security against unauthorised use, destruction of or damage to the information.* This principle requires you to keep personal information secure, including setting the correct policies and procedures. It also requires you to be clear about who looks after personal information and how you would respond to a data breach.

GDPR does mean that you should be able to evidence your compliance with the above principles, if necessary. This can be in the form of documented policies, processes, records and minutes of meetings.

3. The Rights of Individuals

The rights of individuals will change under GDPR, with the following relevant rights implemented from 25th May:

a) *Right to be informed.* Individuals have a right to be informed about the collection and use of their personal information, including what the information will be used for and who else you may share it with (if necessary). They must also be informed of their rights in respect of your processing of their personal information. This can be provided using the aforementioned privacy notice.

b) *Right of access.* This means that individuals can request confirmation that their information is being processed and ask to see the information that you hold on them. Such a request can be made verbally or in writing and must be responded to within one month. Under GDPR you ***cannot*** charge a fee for doing so.

c) *Right to rectification.* Similar to Principle 2d above, you must update information which an individual tells you is incorrect or incomplete.

d) *Right to erasure.* This introduces a right for individuals to have their information erased in certain circumstances. For further detail on when this may apply and how you can handle such a request, please see the following guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

e) *Right to restrict processing.* This allows individuals to request restrictions on the use of their personal information, limiting what you can use their information for. For further detail on when this may apply and how you can handle such a request, please see the following guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/.

f) *Right to data portability.* This entitles people, in certain circumstances, to move, copy or transfer personal information from one source to another. In this case, information must be provided free of charge and in a format that is easily transferred. For further detail on when this may apply and how you can handle this, please see the following guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

g) *Right to object.* When an individual requests that you stop processing their information. This could be because it is being done unlawfully, or because it is being used for a purpose that it was not intended, such as direct marketing. For further detail on when this may apply and how you can handle this, please see the following guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

It is worth noting that many of these rights are conditional. If you are in any doubt at all about when one may apply, seek advice from a qualified authority/expert.

4. Special category data

GDPR has more stringent requirements around handling what it calls “special category data”, defined as information about a person’s: race; ethnic origin; political opinions; religion; philosophical beliefs; trade union membership; genetic data; biometric data; health data; sex life; or sexual orientation.

Therefore, if you have information, for example, about a member’s disability (so you can put in place any special requirements that they may have) then, as a not-for-profit organisation you can only handle that information provided it is not disclosed to any third party, unless you have the person’s explicit consent to do so. For further detail on this, please see the following guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

Similar restrictions apply to information about a person’s criminal history.

5. Children

GDPR recognises that children need particular protection and there are a range of special requirements for processing personal information about children, for example a child aged under 16 cannot give consent, only a parent/guardian can do so (this

age is likely to be reduced to 13 under the UK Data Protection Bill currently before Parliament). For further detail on this, please see the following guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/.

5. Data breaches

GDPR requires organisations to report certain types of personal data breach (e.g. loss, damage to or destruction of personal information) to the relevant supervisory authority, within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. Records must be kept of any personal data breaches, regardless of whether you are required to notify. For further detail on this, please see the following guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

Next steps

There are a number of steps that you can take to prepare in advance of May 25th:

1. Undertake a data and information audit. This will involve noting what personal information you hold, about who, for what purpose and where you hold it. This allows you to determine your legal basis for processing and improve security and access to such information, as well as destroying any personal information that you can no longer justify retaining.
2. Appoint someone to be responsible for data protection and GDPR
3. Consider amending and, if necessary, re-issuing privacy statements.
4. Update any consent requests, if necessary, to make them positive opt-in.
5. Review personal information held in digital locations. This information should be protected, potentially through the use of passwords or unique log in to a secure site. You also need to be sure that the provider of your digital storage complies with GDPR, in particular by not using servers outside the EEA (GDPR prohibits the transfer of data outside the EEA in most circumstances).
6. Maintain records of anything you are doing to comply.
7. Train relevant people, such as volunteers or staff, in your own data policies and procedures, as well as the basics around GDPR.

Appendix

Private Notices / Statements

A privacy notice must be supplied to the individual at the time they provide you with their personal data. The GDPR says that the information you provide to people about how you process their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

Here are some examples of how you can word a privacy notice:

Example 1

How information about you will be used

We will share your information with the Royal Scottish Country Dance Society (RSCDS) for the purposes of administering your RSCDS membership. We may also share your information with {insert as required} for the purposes of {insert as required}.

Example 2

We would like to send you information about club products and events by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant box below.

Example 3

Here at {enter club / branch name} we take your privacy seriously and will only use your personal information to administer your club / branch membership with us. However, from time to time, we would like to contact you with detail of other events / services / offers. If you consent to us contacting you for these purposes, please select from the following options to say how you would like us to contact you.