General Data Protection Regulations

Introduction

As many of you are aware, the law governing the holding of personal data is changing. The General Data Protection Regulations (GDPR) are a Europe-wide set of regulations that come into effect on 25th May 2018 and are the biggest change to data protection law in twenty years. Under the current Data Protection Act, there is an exemption for organisations that hold data for hobby or pastime activities. This no longer applies under GDPR so the whole of NAFAS, nationally, Areas and clubs will now have to comply. And if you were hoping that GDPR, as a European piece of legislation will be swept away on Brexit day next year, I'm afraid that I have to disappoint you since the UK will undoubtedly want to remain compliant so as to ensure minimal disruption to the flow of data between ourselves and the European Union.

Main principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 requires that personal data shall be:-

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Translation!

What all of this means may be summarised as follows:-

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data and who it will be shared with if anyone. This is called "privacy information".

You must provide privacy information to individuals at the time you collect their personal data from them.

Data subjects specifically have to give their consent to their personal data being used; a tick-box indicating that they wish to opt-out is no longer acceptable.

If you obtain personal information from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

The information you provide to people must be concise, transparent, intelligible, easily accessible and it must use clear and plain language.

You must regularly review and where necessary update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.

You must ensure that appropriate technical and practical measures are taken to ensure the security of the data that you collect so that it cannot be used in an unauthorised or unlawful way and that it is protected against accidental loss, destruction or damage.

The penalties for a breach of the GDPR are significant and very much higher than any of the sanctions under the Data Protection Act. Should a breach occur, you have 72 hours to report it to the Information Commissioners Office.

There are six lawful bases for processing data. They are:-

Contractual – the processing is necessary for undertaking a contractual responsibility
Consent – the individual has given clear consent for the use of their personal data
Legitimate Interests – the processing is necessary for your legitimate interest
Legal Obligation – the processing is necessary for you to comply with the law
Vital Interests – the processing is necessary to protect someone's life
Public Task – the processing is necessary for you to perform a task in the public interest

I do not propose to go through each of these as four of them are clearly not applicable to our activities. I believe there is a case for arguing that Legitimate Interests could cover the activities of a membership organisation such as ours; however I do not think that it is strong enough to be certain of our compliance and the hoops through which you need to jump to are complicated, consequently I would rather that everyone signs up with their Consent to be certain of satisfying the law.

The data subject has the right to withdraw their consent at any time and must be made aware that they have this right before they give their consent. If consent is withdrawn, you will have to delete the data records you hold on that subject within one calendar month.

On request you must give the data subject copies of the personal data that you hold on them within one calendar month at no cost.

The permission may be in the form of a signature on a membership form for instance, or a tick box in a reply to a personal email. This permission must be recorded as evidence should there ever be an investigation.

Particular and specific permission is required if holding an event, where photographs are taken and may be published, and a form for permission signatures with a notice of explanation should be at the entrance. Verifiable verbal consent is acceptable in some circumstances such as at a club meeting when a demonstrator allows the use of photographs of the demonstration for club or personal use but not for public wider use eg social media, the internet or printed publishing.

Now to the logistics of this for the Area and Clubs

To comply for the current year the Area should send an email explaining the reasons to the officers of each Club, Individual Members, Demonstrators, Tutors Judges and Speakers, requesting permission to hold and use their data by ticking a box and returning the email. Those not on email should receive the request by post and give permission with a signature on a tear off attachment. How the information is to be used will be specified for each category as it will differ – for example the contact details of the secretary or other nominated club officer would be published on the Area Club lists and/or the website, and could also be given to potential new club members by an Area Officer.

For subsequent years the request will be included in renewal forms. While this is an annual process, we should give a retention time of three years so that there is no chance of a data breach because of a delay in sending the forms out or receiving replies.

It would be sensible for clubs to do the same, although the statement at the point of consent will be simpler for clubs as the information is normally held only for purposes of communication of club and Area information.

It is important to emphasise to Area/club members that if they do not reply, they will no longer receive any Area/club information.

A possible club permission statement could be:

I agree that the committee of …….. club may hold my personal data, by automated or other than automated means, for the purpose of communication of Club and Area matters. This information may be held for a period of no more than three years and will be deleted if I am no longer a member of the Club or request that the details be deleted.

Name (printed) …….. Signature …… Date …….

If you have a club Facebook page or website with contact details, specific permission must be held from that person.

Suggested wording for Area forms.

Individual Membership

I agree that the officers of the …….. Area of NAFAS may hold my personal data, by electronic or other than electronic means, for the purpose of communication of Club and Area matters. This information may be held for a period of no more than three years and will be deleted if I am no longer an Individual Member or request that the details be deleted.

Name (printed) …….. Signature …… Date …….

Club Officers

Chairman

I agree that the officers of the …….. Area of NAFAS may hold my personal data, by electronic or other than electronic means, for the purpose of communication of Club and Area matters, to be included on the Area Club list. This information may be held for a period of no more than three years and will be deleted if I am no longer the club chairman or request that the details be deleted.

Name (printed) …….. Signature …… Date …….

Secretary

I agree that the officers of the …….. Area of NAFAS may hold my personal data, by electronic or other than electronic means, for the purpose of communication of Club and Area matters, to be included in the Area Club list and on the Area web site, and given to potential new club members. This information may be held for a period of no more than three years and will be deleted if I am no longer the club secretary or request that the details be deleted.

Name (printed) …….. Signature …… Date …….

Treasurer

I agree that the officers of the …….. Area of NAFAS may hold my personal data, by electronic or other than electronic means, for the purpose of communication of Club and Area matters, to be included in the Area Club list. This information may be held for a period of no more than three years and will be deleted if I am no longer the club treasurer or request that the details be deleted.

Name (printed) …….. Signature …… Date …….

JDSE

I agree that the officers of the …….. Area of NAFAS may hold my personal data, by electronic or other than electronic means, for the purpose of communication of Club and Area matters and to be included in the Area JDSE list, which will be circulated to Area Clubs and supplied to other club or individual members of NAFAS on request. This information may be held for a period of no more than three years and will be deleted if I am no longer an Area JDSE member or request that the details be deleted.

Name (printed) …….. Signature …… Date …….

Contact Cards – exhibtions/shows etc

I agree that my personal details may be held by the officers of the …….. Area of NAFAS for the purpose of putting me in touch with a flower club. This information may be held for a period of no more than two years and will be deleted earlier on request.
Name (printed) ……. Signature …… Date …….

These forms are just suggestions and can be changed so long as the basic principles are present to whatever format you and your clubs feel is appropriate.

I will be very happy to receive thoughts, comments, suggestions and (helpful) criticisms.

May I express my thanks to Sheila Tasker of London & Overseas Area for her help in compiling this report and for permission to use some of her text and form layouts.