Amphibian and Reptile Groups of the United Kingdom

ARG UK Advice Note 9

www.arguk.org

The General Data Protection Regulation (2018) for volunteer groups
February 2018

Background

On 25th May 2018 the new General Data Protection Regulation comes into force. This is not a new legislation, as it builds on the Data Protection Act 1998. Nevertheless, it represents an important challenge for volunteer groups, since there will be greater scrutiny of the way in which we manage personal information after this date.

Definition of Personal Data

Any information relating to a natural person, who can be identified, directly or indirectly, by reference to:

- Their name, identification number, location data, online identifier
- one of more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity

Even volunteer groups like the ARGs have to take responsibility for the personal data we hold. For ARGs this could include: names, contact details (address, email, phone no etc), medical details, other personal details.

An EU level response to issues arising from the greater use of technology, and the opportunities for loss or theft of data:

- the rise of social media and sharing of personal information
- the extended use of 'smart' mobile devices, and laptops for hot desking and home working
- greater use of mobile banking and internet shopping
- recent well publicized data hacks e.g. Talk Talk, NHS, leading to potential data theft and fraud

It is our responsibility to protect the data we hold in a secure and transparent way that respects the rights of the individual.

What does this mean for the ARGs?

This means that volunteer groups like the ARGs have to take responsibility for the personal data we hold. For ARGs this can include:

- contacts (by email, mail and phone)
- volunteers
- members
- project partners or other associates

- funders
- enquiries

Under the new law any form of data processing requires ONE of the following:

CONSENT

Freely Given
Reversible
Informed
Enthusiastic
Specific

- The consent of the data subject
- It must be necessary e.g. for the performance of a contract, or compliance with a legal obligation (e.g. insurance)
- It must be necessary to protect the vital interests of a data subject (e.g. keeping emergency contact details, medical and next of kin information)
- It must be necessary for the performance of a task carried out in the public interest
- Necessary for the purposes of legitimate interest

Legitimate interest is important as it will enable you to continue to contact those who would reasonably expect to hear from you, for example: members, supporters, volunteers, funders and other ARGs.

This is a slightly gray area, and in order to comply we must:

- Balance the needs of legitimate interests to process personal data against the individual's right to privacy
- Make a record of this assessment
- Be able to explain why we are collecting the information e.g. membership, records, to put on a newsletter list and what legitimate interests we are relying on to maintain and use the data.

Note: Individuals have greater rights to object to processing of their personal data under legitimate interests. The onus is on the organisation to demonstrate that their legitimate interests outweighs the privacy of the individual, or you must remove that individual from your data base.

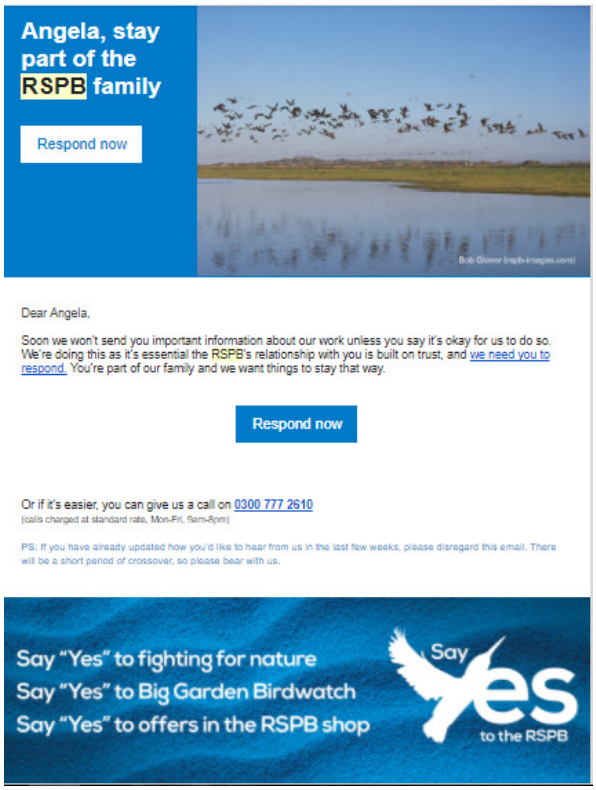
Process for complying with the new GDPR:

1. **Appoint or identify a Data Protection Officer**: Each ARG needs to identify a Data Protection Officer: who will take responsibility for making sure that personal data is managed in line with the new GDPR.
2. **Create an Information Asset Register:** This is a record of what and how personal data is held and processed. For each personal data record you hold you need to work out:

   - Why you have it – and what the basis of this is (i.e. did the subject originally agree to you having it)
   - Where do you keep it e.g. on computer, phone, data stick, paper file
   - Where did you get it from e.g. the individual directly or via a third party
   - How long have you had it for – how long do you intend to keep it for, is the individual aware of this
   - Is it up to date – when did you last check
   - Risk – are you keeping this information safely, what could go wrong

   We have been asked about **Record Pool**. Personal data is held in an encrypted form on record pool, and since September 2017 local recorders can no longer routinely access this. Verifiers can access personal information such as email addresses, but only for the purpose of checking for (i) known or trusted recorders, or (ii) contacting the originator for verification purposes. Personal information (recorders'

names and emails) must not be downloaded and circulated to third parties, but all records have a unique ID, which can be used.



3. **Existing contacts:** contact everyone on your lists, explain why you are doing this (due to changes in data protection regulations), and ask them for their consent to remain on your lists. One way of doing this is by sending your emails through an automated service such as mail chimp (https://mailchimp.com). This can have an 'opt in' button prominently displayed, so that people can easily give their consent. We have given the example of the RSPB as an example.

4. **New contacts:** When you collect new personal data, ask people to 'opt in' to further contact, be clear about:
   - how and when their information will be used,
   - where you will keep it,
   - who you will share it with,
   - what security you have in place for it, and
   - how long you will keep it for

5. **Data limitation:** An important part of the process is being clear about why you are keeping personal information. Ensure that you only hold the information you need, and no more than you would require for the purposes for which you have told them you will use it. If information is not relevant e.g. on former members or volunteers, you should delete it. If they return, then you can always ask them for it again.

6. **Accuracy:** Personal data must be up to date and accurate. Inaccurate personal data should be corrected or deleted in a prompt manner.

7. **Storage limitation**: Personal data should be kept for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes), and should be permanently deleted or anonymized as soon as it is no longer required. Always make sure that people know what will happen to their data when they no longer wish to be contacted.

8. **Integrity and confidentiality**: Personal data must be held in a secure manner. This is a particular issue with electronic records, which could potentially be accessed from a lost (or stolen) laptop or smart device. We recommend that all personal data is password protected, and preferably encrypted.

New Security Obligations under GDPR:

- Personal data held in the public domain should be encrypted and/or anonymized;
- The ARG must have the ability to ensure that personal data is held in a secure, confidential and resilient manner. Breaches most often occur, where personal data is in transit or on home devices where security systems may not be as effective as in a professional situation;
- Personal data is held securely and can be readily restored; and
- Data security arrangements are monitored and tested to ensure that security and back up processes are effective

9. **Cloud computing:** Many of us are moving to 'cloud based' computing to store our documents and emails. In some cases this may mean that personal data is being held on servers that are physically located in another country, and may not be subject to the same standards of security and protection. It is your duty under the new law to ensure that the service you are using complies with the law. Many providers (i.e. Amazon Web Services, Microsoft, IBM Cloud and Google Cloud) are incorporated in the USA, and you need to make your contacts aware of this.

Definition of Personal Data Breach

A breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Breaches can occur for many reasons, but the most common are set out here:

- Email inadvertently sent out without bcc: function
- Staff using own devices
- No password / weak password / password on a post-it stuck to the computer
- Working on the move / working at home
- Loss of unencrypted device (smart phone, lap top, data stick).
- People accessing information they don't have the right to see
- Lack of back-up / no testing of back-up
- Hacker
- Phishing
- Unsecure website
- Providing information to the wrong individual
- Theft of data
- Inappropriate user-permissions

Any serious data breach must be notified to ARG UK, immediately who will determine how to proceed. This may include reporting the breach to the individuals affected and the Information Commissioners Office (ICO).

This Advice Note was first published in February 2018, based on the information provided in a training workshop run by the Oxfordshire Community and Voluntary Action (OCVA) in October 2017, and discussions held at a workshop run at the 2018 HWM by Angie Julian and Chris Monk. We are grateful to all the participants of Workshop E for their support.

This current version can be downloaded from the ARG UK website www.arguk.org and should be cited as: ARG UK (2018): ARG UK Advice Note 9: The General Data Protection Regulation (2018).