

# Biological Recording and Data Protection

Author: Paul Gilbertson, Joint Nature Conservation Committee

Date: 15<sup>th</sup> May 2018

## Introduction

This document attempts to set out a clear route for a wide variety of bodies towards compliance with the new Data Protection Act and the General Data Protection Regulations. It is the product of the author's reading of relevant legislation, guidance, and conversations with the NBN's Data Protection Group.

---

*This document does NOT constitute legal advice. Each organisation must make a judgement for itself on the steps they will take.*

---

## General Advice

Different sizes of organisation are expected to do different things. Actions taken should be proportionate to your organisations size and resources. The Information Commissioner's Office (ICO), who handle data protection enforcement and regulation in the UK, are not expecting tiny volunteer charities to employ specialists.

May 25<sup>th</sup> is not a deadline, but the start of the journey. Have a plan of action to put further steps in place and carry it out in a timely manner.

## What is Personal Data, and what data do we hold that might be Personal Data?

The ICO has issued guidance in determining if a piece of data can be classified as personal data:

- Can a living individual be identified from the data?
- Does the data relate to the identifiable living individual, in the capacity of family, business or profession?
- Is the data evidently about a particular individual?
- Is the data 'linked' to an individual so that it provides specific information about them?
- Is the data used, or to be used, to inform or influence actions or decisions affecting an identifiable individual?
- Does the data have any biographical significance in relation to the individual?
- Does the data focus or concentrate on the individual as its central theme?
- Does the data impact or have the ability to impact the individual in the capacity of family, business or professional or personal?

A living individual could be identified with the information linked to a biodiversity record, with particular emphasis on;

- Can a living individual be identified from the data?
- Does the data have any biographical significance in relation to the individual?

Under the Data Protection Act guidance issued by the ICO one of the tests used to determine if data is personal is called the 'Biographical Significance' test:

*"Where an individual is listed as an attendee in the minutes of a meeting then the minutes will have biographical significance for the individual in that they record the individual's whereabouts at a particular time."*

## Biological Records

Whilst a biological record at minimum consists of three main elements, species, position, and time, most biological records contain the recorder name as a fourth element. The recorder name is used to aid verification of the record for quality purposes. In addition to recorder, a record may optionally contain determiner and verifier names. These are considered of less value to the general user.

**A biological record clearly identifies a person at a potentially specific location and day. Even though the person is not the subject of the record, it constitutes personal data.**

In addition, the information may be combined with other information such as a list of people with an expertise in a taxon group or a list of people and their addresses (eg Edited Electoral Register) which could enable identification of a specific individual.

**Anonymised biological records (those without names) are not personal data.**

## Volunteer Details

Some groups also collect detailed data on volunteers in order to communicate with them for verification purposes. Where detailed data is collected purely for these purposes, it should not be used for marketing or advertising purposes. It is better to be clear about the purposes for which you collect the data, and where possible allow volunteers to opt-in to such communications.

**Volunteer details can be collected alongside biological records and count as personal data.**

## How do you create a Personal Data Inventory?

Each organisation should identify where they hold personal data, how they collected it, the legal basis for holding the data, and how they are going to action the various rights individuals have. It is recommended that a Personal Data Inventory is created to hold this information. For smaller organisations, a simple spreadsheet should suffice.

The rest of this document should help with filling out this inventory, and the process of doing so will help in identifying steps you need to take.

## What rights can we use to collect data?

The General Data Protection Regulation enumerates a number of rights upon which organisations can rely on for collecting personal data. These are:

- Contract
- Legal Obligation
- Legitimate Interest
- Public Task
- Vital Interests
- Consent

For biological records, only four of the bases are relevant and are detailed below.

### Public Task

Government Departments, Local Councils, and associated Public Bodies, can utilise the Public Task basis when processing personal data in line with their statutory functions laid down in domestic or EU law, or associated with an international treaty.

**For nature conservation bodies, almost everything done with biological records is related to statutory functions, so the Public Task basis should be used in preference to other bases.**

Other non-public bodies which are carrying out statutory functions may also utilise this basis when directly carrying out a public function. In this area, this might apply to some Local Record Centres carrying out searches on behalf of Local Authority planning teams. It depends on the nature of the relationship, and Contract may be a better basis, please seek legal advice if necessary.

### Contract

When an organisation is processing personal data on behalf of another organisation, who has a legal basis for having the data processed, then the Contract basis allows the contracted organisation to hold and work with the data. They can only hold the data whilst performing the contract, and can only work with the data for the purposes of performing the contract. If the organisation wishes to use the data for other purposes they will need to acquire the data again separately under a different basis.

**For Environmental Consultancies, Local Environmental Record Centres, NGOs, and other organisations that are contracted to perform surveys, then Contract is the correct basis for processing. It does not apply to collaborative efforts where one organisation is not directly paying another to perform the task.**

### Legitimate Interests

The Legitimate Interests basis allows organisations to collect and process personal data as part of their normal conduct of business. For the most part, non-public bodies will use this basis for the majority of work with biological records. The basis is not a carte-blanche however, organisations need to demonstrate and record the interest they are trying to serve, ensure there is no reasonable way to do it without the personal element and balance up the privacy rights of people with their needs as an organisation.

To do this, organisations should perform a Legitimate Interests Assessment (LIA) and keep it as part of their records. For advice on how to perform a LIA and a template document visit the ICO website at: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>

**For most biological recording the requirement for personal data is around verification of records. Having recorder details allows verifiers to contact them with regards to their records. Legitimate interests should be avoided when using details for external marketing purposes as marketing can be done without holding personal details, Consent is the correct basis for this.**

### Consent

The Consent basis remains for when a requirement fails the Legitimate Interest Assessments. Under this basis affirmative and active consent is requested from the data subject. This means that forms should include tick boxes for each activity you are seeking consent over. You must also allow people

to withdraw consent at any time for any reason, and once they have, delete their details from systems.

Access to services and functions cannot be predicated on consent, and users who give consent should be treated the same as users who do not. If a particular service requires the information to function then Legitimate Interests would be a better basis.

**If you have previously gained consent in a manner that is compatible with the principles laid out above, you do not need to ask for consent again.**

## What is a Privacy Notice? Do we need one?

When you collect data, at the point of collection, you need to present the person whose data you are collecting with a Privacy Notice. This notice needs to detail (at minimum):

- Who you are
- What data you are collecting
- Which legal basis you are using
- Why you are collecting it, and what you are doing with it
- How long you will need to keep it for
- Who you will be sharing it with
- How you are handling subject rights

The retention period for data details how long you will keep the personal data for. Organisations need to determine for themselves how long they feel comfortable with retaining the data. For recorder names an indefinite period is considered justifiable as there is an exception for data that becomes part of the Scientific Record. Contact details for recorders would likely need to be retained for a limited period after verification is completed, with a maximum retention period of 10 years in the event that the record is never verified.

An example Privacy Notice for a fictional recording scheme is included in Annex A.

**Multiparty collaborative national monitoring schemes that JNCC assists will be receiving separate advice and Privacy Notices in due course. There are a number of very specific tweaks that need to be considered in each case. For other similar groupings, seek legal advice.**

## What rights do Data Subjects have?

The new Data Protection Act grants new rights for people to exercise in regards to privacy. This section will not fully detail these rights, but instead focus on how they apply to biological recording.

### Right of Access

People have a right to know what information an organisation holds on them. For biological records this means access to the records for which they are the recorder or determiner/verifier, along with other information the organisation may hold. Such a request can be made in any way, to any organisation employee, not just the contact point specified in the Privacy Notice.

**For biological records, where this is held in electronic form, then it should be provided as a Excel or CSV file. This must be provided free of charge and within one month of receiving the request.**

If an individual makes multiple repeated requests then an organisation has the right to ignore these requests as excessive, or a charge to cover the full administrative cost.

## Right of Erasure

The right for someone to 'be forgotten' now exists in specific legal form. People can ask for organisations to erase data they hold on them. This right can be exercised in any way, to any organisation employee, not just the contact point specified in the Privacy Notice.

If you are using Consent as the basis for processing the data, you must erase the data, inform all others you have passed the data to that they must do the same. For Public Task, you may refuse the request in writing.

**Biological records can be considered as part of the scientific record, a specific defence in the GDPR, if the legal basis is Contract or Legitimate Interests. This would not apply to volunteer contact details nor other marketing data.**

Organisations must action the request within one month.

## Right to restrict processing

People who have specific circumstances that mean they would be unduly burdened by otherwise legal uses of their data may request that the usage stops. Each organisation must individually weigh up the circumstances of that individual with the tasks at hand. Refusing such requests should be made clear and pass the 'reasonable person' test.

If after agreeing to the request, you no longer have a reason to use the data, it must be erased.

## What about children?

Whilst the GDPR specifies children as being under the age of 18, Her Majesty's Government has revised that to be under 13 for the purposes of UK Law. Children get special additional protections including Privacy Notices written in a form understandable by them, and the need for parent or guardian consent.

**If an organisation is knowingly embarking on a project involving children, or processing child data, they should seek specialist legal advice.**

## What should we do if there is a data leak?

People have a right to expect their data will be kept secure. Organisations should take reasonable steps to ensure technical measures have been put in place. Where possible encrypted devices should be used, firewalls and anti-virus software installed, and software patches applied. Also all staff must be trained in how to handle personal data.

**In the event that someone has access to the data, either through hacking or employee error, you must inform the Information Commissioner's Office. This must be done within 72 hours of being notified of the leak.**

## Can we share data?

Yes, where it is necessary to undertake the tasks outlined in the Privacy Notice. Organisations should have a data sharing agreement with any organisation they are sharing data with. This agreement should outline the uses to which the data can be put.

**Anonymised records are not personal data, so can be shared freely.**

## Can we celebrate significant records?

Organisations may wish to inform readers about significant records, or celebrate milestones, and provide the recorder name as part of that news piece. Organisations may do this as long as the record position and time is sufficiently generalised. There is a general exception for journalism and newsletters, annual reports and so forth would fall under this.

## What about Open Data?

Publishing full records with recorder names under GDPR may have issues. If the organisation feels that it has a Legitimate Interest that passed the LIA to include those names then it may do so. Such a position would need to apply to all records, not on a opt-in/opt-out basis.

For most organisations who have traditionally offered an opt-out for recorder names being part of the public records, this would be using the Consent basis. It is unclear that the difficulty of withdrawing consent from an open data dataset would be allowed under the Regulation and new Act.

**We are still seeking advice on this issue and will update this accordingly. Organisations should either await further information, or seek independent legal advice. We are also investigating what data users of Open Data need to do when they wish to use records with names in.**

## Annex A: Example Privacy Notice

### Privacy Notice

Version 2; last updated 18/05/2018

#### **Who are we?**

Fluffy Bunny Study Society is a charity dedicated to the study and preservation of *Bunnica Flufficus* a particularly rare and fictional species of rabbit. Founded in 2009 in order to stress test the now defunct NBN Gateway, we rely on volunteers to help advance our studies and promote the plight of fictional herbivores and the electronic environments in which they thrive. We are registered charity no. 9999999 in England.

#### **What are we collecting your information for?**

FBSS is collecting your personal data in order to help map the extent of *Bunnica Flufficus* in the UK and Ireland. We are collecting your contact details in order to help verify records that you submit to our recording project. To do this we require your name, address, email address and telephone number. One of our verifiers may contact you if we need to discuss any particularly interesting records you submit. We feel we have legitimate interest to do so. We will keep this information for 7 years.

We would like to provide you with further information regarding the 'Soft Rabbits are Great' conference on 31/02/2029, and make arrangements to accommodate delegates including any dietary or access requirements. This processing can only be progressed with your consent. We will delete this information within one month of the conference concluding.

We would also like to provide you with further information of interest to *Bunnica Flufficus* recorders and the FBSS activities. This processing can only be progressed with your consent.

#### **Where are we storing your information and will we share it?**

Your personal data will be stored on FBSS's internal servers and your contact details will not be shared with any other organisation except as a legal requirement and will not be transferred outside of the EU.

We may share records you submit with partners and other nature conservation societies in the interests of wider nature preservation. These records will include your name as the recorder, but no further contact details. We will ensure that these partners keep your information secure through Data Provider Agreements.

Anonymised versions of records will also be released as open data on the NBN Atlas.

### **Your rights and our contact details**

You are entitled to access any of your personal data which we hold. If you wish for us to send you a copy, please contact [data@fbss.fakedomain](mailto:data@fbss.fakedomain) with as much detail as possible on the information you would like us to provide, and we will respond within one month.

You have the right to object to the processing of your data. You also have the right to request that we restrict or stop processing, rectify or delete your data. Where the data we hold has not been supplied by yourself, you are entitled to ask how we obtained the data. Please contact OUR data Coordinator at [data@fbss.fakedomain](mailto:data@fbss.fakedomain) if you wish to progress any of these rights in this case.

If you have any concerns about how your data is being used, we will endeavour to answer any questions you have. You have the right to [lodge a complaint](#) with the [Information Commissioner's Office](#). You also have the right to an effective judicial remedy against decisions of the Information Commissioner's Office, or against FBSS.