# GENERAL DATA PROTECTION REGULATIONS

## INTRODUCTION

Data Protection law in the UK will undergo some significant changes with the introduction of the General Data Protection Regulations (commonly referred to as the **GDPR**). The GDPR will replace the current Data Protection Act from 25 May 2018. (The Government has confirmed that "Brexit" will not affect the GDPR from coming into effect so you cannot ignore it.) The changes require some planning and may require changes in our forms and procedures.

These guidance notes are to be regarded as the Policy for Basildon Borough Heritage Society whilst also giving an overview of how the General Data Protection Regulations are to apply to societies, associations and recognised centres for the purpose of the function of being a recognised centre. The uses you make (and want to make) of the information about living individuals which you obtain will be governed by the GDPR and this as our Policy Document. Failure to comply with the GDPR will attract very much higher penalties than now.

## DEFINITIONS

The General Data Protection Regulations relates to **personal data** and **special categories of personal data**.

### Personal data

Any information relating to an identified or identifiable natural person (referred to as the **Data Subject**).

A person is identifiable if they "*can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors, specifically the physical, physiological, genetic, mental, economic, cultural or social identity of that actual person*".

### Special categories of personal data (Sensitive personal data)

Personal data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

The special categories of personal data do not include personal data relating to criminal convictions and offences but there are similar extra safeguards in relation to those types of data.

## Processing

"A*ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, determination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

### Data Controller

*"The natural or legal person, public authority, agency or other body which, alone or jointly, with others determines the purposes and means of the processing of personal data"*.

### IN PRACTICE

Most, if not all, the information requested on membership application forms, event entry forms and which you collect from visitors, suppliers, staff and volunteers will be personal data. That will include names, addresses, dates of birth, telephone numbers, and e-mail addresses. However, personal data can also include opinions held about someone and can include references to them in emails or other communication. Information about health and physical disabilities will be sensitive personal data to which additional safeguards apply.

Given the extent of the definition of "processing", you should assume that any use you make, or want to make, of the personal data, as well as your collection, storage and destruction of it, will be governed by the GDPR.

### NOTIFICATION / REGISTRATION

The requirements for organisations to "register" with the Information Commissioners Office (ICO) is being removed by the GDPR and replaced by the general accountability obligation to demonstrate compliance with the data protection principles.

### DATA AUDIT

The GDPR is a more extensive piece of legislation than the existing Data Protection Act. However, as we are already complying with the Data Protection Act, we are likely to be well on the way to compliance with the GDPR.

We have established that our current policies and procedures are suitable to comply with the GDPR and have reviewed and altered them, where necessary, to suit.

**We have assessed:**

- what personal data we hold;
- whether it is needed;
- where it came from and the basis on which it was collected;
- what you do with it and are planning to do with it;
- where and how you store it.

**This is documented in the Office Management file.**

We may have obtained the consent of the individual to whom the data relates when originally collected. If so, they should have been told at the time we collected the data, what we would use it for.

If we cannot clearly identify that we have consent (in accordance with the GDPR) then we should consider whether we can use the data on one of the other bases of processing (see section **Collecting and Keeping Data**). If not, then we will have to collect the data again, with the appropriate consent request.

The most convenient time to do this is on renewal of the individual's membership but if that is after 25 May 2018 we need to be aware that we risk not being compliant with the GDPR.
It is very important that the data is only used for the purposes which were made clear to the individual at the time the data was collected. We cannot, therefore, collect data for the purposes of managing a member's membership and then use it for other purposes.

**ACCOUNTABILITY AND GOVERNANCE**

The GDPR makes the principles of accountability and transparency far more significant than under the Data Protection Act. We must be able to demonstrate that we comply with the data protection rules.

There are specific obligations on maintaining records which apply particularly to organisations with 250 employees or smaller organisations where the processing is not occasional or includes sensitive persona data or is likely to result in a risk for the rights and freedoms of the data subject. Whilst the obligation to maintain records is unlikely to apply to the majority of Basildon Borough Heritage Society affiliated organisations we advise:

**A prudent approach is to have a data protection policy which records:**

- the purposes of the processing;
- the categories of data subject and the categories of personal data which relate to them;
- the recipients / categories of recipients of the personal data;
- any overseas transfers of the personal data;
- general indication of time limits for erasure of the different categories of personal data;
- description of technical and organisational security mechanisms you use.

Such information should be identified in any event in order to decide what steps are needed to be taken to comply with the GDPR.

Whilst it will not be mandatory for Basildon Borough Heritage Society to appoint a Data Protection Officer it would be prudent for someone to take ownership of the role. Appointing someone within the organisation to take ownership of the process is likely to be necessary.

Data protection rules are enforced by the Information Commissioner. The Information Commissioner's Office (ICO) has a website (ICO.org.uk) which contains very useful information. This Guidance Note contains links to some of that guidance which is likely to be particularly relevant.

**Kenneth F. Porter**
**Chairman**
**Basildon Borough Heritage Society**