

# ***The Data Protection Act (1998)***

## ***Advice for RAYNET groups***

### ***Introduction***

The purpose of this document is to offer practical advice to RAYNET groups on the implications of the changes in the legislation concerning Data Protection. The paper covers the key principles for data protection and offers concrete advice for RAYNET Groups, as well as some background information about the Act.

### ***Background***

The Act came into force at the beginning of March 2000. Key changes under the Act include:

- ***Extending the provision to include manual records***
- A new definition of Sensitive Personal Data
- An individual right to prevent processing likely to cause damage or distress
- An individual right to prevent processing for the purpose of direct marketing
- New exemptions from notification and registration
- ***A direct requirement on data controllers to comply with the data protection principles **whether they are required to notify under the Data Protection Act or not.*****
- The Data Protection Registrar will now be called the Data Protection Commissioner and has powers of enforcement and a new duty to promote good practice.

### ***Eight Data Protection Principles***

All Data Processors and Data Controllers must adhere to the following principles that data must be:

1. Processed "fairly and lawfully"
2. Obtained for a "specified and lawful purpose"
3. Adequate, relevant and not excessive to that purpose
4. Accurate and up to date
5. Kept only for as long as required for the purpose for which it was obtained
6. Processed in accordance with the rights of data subjects
7. Secure - the level of security being proportionate to the level of harm that could result if unauthorised access occurs
8. Not transmitted outside the EEA without consent from the data subject

### ***Rights of Data Subjects***

Data Subjects have the right:

- To know that the information is held and the purpose for which it is held
- To stop any automated processing (e.g. express that no data is held in computer system)
- To stop processing likely to cause "substantial damage or distress"
- To receive prompt replies to queries concerning data held about the subject. (If requests are received from data subjects, copies of their records must be made available within 40 days.)
- To prevent processing for the purposes of direct marketing.

## **Exemptions**

Registration is now called notification and an exemption from notification has been provided for small clubs, voluntary organisations, church administration and some charities. This applies to RAYNET groups if your processing is only:

“For the purposes of establishing or maintaining membership or support for an association not established or conducted for profit or providing or administering activities for individuals who are either members of the body or association or have regular contact with it”

All those processing and using data on behalf of a RAYNET group need to abide by the eight data protection principles and ensure the rights of data subjects are upheld.

Under this exemption you may only:

- Hold and process data necessary for the exempt purpose
- Disclose to 3rd parties which are necessary for this exempt purpose

## **How this applies to RAYNET**

Until now, groups could avoid registration under the ‘unincorporated members association’ exemption clause, providing they only held data on their own membership and only disclosed within the group. If any other contact details were held or disclosure required, registration was required. This clause, along with many others, no longer exists in the 1998 act.

Under the 1998 act, other contact details (such as user services, event organisers etc.) and other external contact information can now be held without the need to notify, as it is deemed to be “providing or administering activities” for the group.

The new disclosure clause under the not-for-profit exemption allows you to provide information, as needed, to members of the user services and other agencies involved in our activities.

Groups must have a defined mechanism for requests from Data Subjects for disclosure of information held on them. This disclosure must be in full (including all sensitive personal data), written and provided within 40 days of the request.

***Remember that you may not need to notify your data usage, but you cannot escape from the requirement to comply with the principals of the Data Protection Act.***

## **What is sensitive personal data?**

Explicit consent is required from a data subject to hold sensitive personal data. Please refer to the glossary for a full list of sensitive data definitions.

Information likely to be held by RAYNET groups includes:

- Health
- Disabilities / special needs

This is information that a responsible group should hold, with the data subject’s consent, as controllers need to be aware of conditions that could affect a members’ ability to carry out duties.

***Groups should ensure that any request for sensitive personal data includes written consent from the member for that data to be held. The data must be kept up to date.***

## **But RAYNET has notified nationally, does this not cover us?**

No, it only covers the Committee of Management and specialist teams.

If this notification were extended to every group, requests for disclosure from a Data Subject would involve checking with every group in the county for details on the member.

Local Group and County data usage is the responsibility of the respective Controllers, who should ensure compliance within their own areas.

## **Glossary of terms**

|                                |   |
|--------------------------------|---|
| <b>Data</b>                    | <p>Information processed by means of automatic equipment (computers, faxes etc.) and/or recorded as part of a "relevant filing system" and/or which constitutes an accessible record.</p> <p>Personal Data about any living individual who can be identified from that data or from any other information held by the data controller.</p>  |
| <b>Sensitive Personal Data</b> | <p>Defined as:</p> <ul style="list-style-type: none"><li>• Race and/or ethnicity</li><li>• Political beliefs</li><li>• Religious and similar beliefs</li><li>• Trade union membership</li><li>• Physical/mental health</li><li>• Sexuality</li><li>• Criminal convictions and offences</li></ul> <p>Names, addresses, dates of birth and telephone numbers are <b>not</b> considered Sensitive Personal Data.</p> |
| <b>Data processing</b>         | <p>Obtaining, recording or holding personal data and "carrying out any operation or set of operations on it."</p>   |
| <b>Data controller</b>         | <p>The person or persons who determine the purposes and manner in which personal data is processed.</p>   |
| <b>Data subject</b>            | <p>Each individual whose information is held.</p>   |
| <b>Relevant filing system</b>  | <p>"any set of information relating to individuals, that... is structured... in such a way that specific information relating to a particular individual is readily accessible" In other words any set of well-kept records whether on computer or not.</p>   |
| <b>EEA</b>                     | <p>European Economic Area (the 15 EU member states plus Iceland, Liechtenstein and Norway)</p>  |