



SCoR

THE SOCIETY & COLLEGE
OF RADIOGRAPHERS

Data Protection Compliance Handbook

May 2018

DATA PROTECTION COMPLIANCE HANDBOOK

Contents

Version Control	1
Introduction	1
Purpose of this handbook	1
How we comply with data protection legislation	2
The personal information that we collect and process	2
How we use personal information	2
Sharing personal information	3
Data subject rights	3
Our data protection operating procedures	5
Responsibility Agreement	7

DATA PROTECTION COMPLIANCE HANDBOOK

Version Control

Version number	Date	Change	Person
6	19 March 2018	GDPR Introduction	Eugene Statnikov
7	03 May 2018	SCoR Additions	Eugene Statnikov

Introduction

This data protection handbook was first issued by The Society and College of Radiographers (SCoR) on 1st February 2003 and subsequently revised in 2018. SCoR assessors, council members, committee members, employees, representatives, and trustees are required to follow this handbook. Failure to do so could result in disciplinary proceedings.

The SCoR are both registered with the Information Commissioner's Office (ICO) as data controllers¹. We have a legal duty under the EU General Data Protection Regulation (GDPR) to protect the personal information² that we collect and process³. GDPR superseded the Data Protection Act 1998 and became effective in May 2018.

Failure to comply with the legislation can lead to criminal prosecution of organisations and persons affiliated to organisations (e.g. staff, representatives, trustees, etc) with fines of up to €20m. Even an investigation of a potential breach by the ICO will on its own damage the reputation of our organisation.

Purpose of this handbook

This handbook, which is relevant to SCoR assessors, council members, committee members, employees, representatives, and trustees, is designed to protect the personal information of our data subjects who are mostly members, beneficiaries, and employees. It is to inform you about the personal information that we collect, how this information may be used, and the procedures you must follow to comply with data protection legislation.

¹ A 'Data Controller' is an organisation which determines the purposes for which and the manner in which personal data is processed.

² 'Personal information' includes personal and sensitive personal data. It is information, facts or opinion, recorded electronically or in mail filing systems, which identifies a living individual. Sensitive personal data is known as 'special categories of personal data' under GDPR. It includes information about someone's health, religion, political opinion or trade union membership, race, ethnicity, or sex lives.

³ The safest way of defining 'Processing' under data protection legislation is to think of it as 'using' personal information. It includes obtaining, holding, recording, retrieval, consultation and the disclosure of personal information.

DATA PROTECTION COMPLIANCE HANDBOOK

How we comply with data protection legislation

The SCoR have a designated “Data Protection Officer” who is responsible for gathering and disseminating information and issues relating to data protection legislation.

We have implemented processes and procedures to help us comply with the requirements of the GDPR. The eight data protection principles or rules require that:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall only be processed for the purposes for which it was obtained
3. Personal data shall be adequate, relevant, and not excessive in relation to its purpose
4. Personal data shall be accurate and kept up to date
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of Data Subjects
7. Appropriate technical and organisational measures shall be taken against unlawful processing or accidental loss
8. Personal data shall not be transferred outside the European Economic Area (EEA) unless the country has equivalent Data Protection standards

We provide data protection guidance and training to SCoR employees, representatives, trustees, council members and assessors so that you are aware and reminded of your data protection responsibilities.

The personal information that we collect and process

We collect and process personal information about our members, beneficiaries and employees. This can include name and contact details, date of birth, nationality and ethnicity, employment information and professional qualifications, bank account details, and other information relevant to your employment service.

Most of the personal information that we collect and use is considered to be sensitive because it is connected to the fact that someone is a member of our trade union.

Our lawful basis for processing this personal information is to manage our membership and fulfil our legitimate interests as a trade union and professional body.

Where necessary we obtain active consent from individuals for processing personal information for other purposes than managing the membership – see below.

How we use personal information

We use the personal information that we collect:

DATA PROTECTION COMPLIANCE HANDBOOK

- To process and manage membership which includes: (this is part of the legitimate interest of the SCoR)
 - Processing membership payments and renewals
 - Providing course and event information
 - Keeping a record of our relationships with members and beneficiaries
 - Managing marketing and communication preferences
 - Providing members with information about us and the work that we do
 - Processing of accreditation
- To represent our members, as a whole, as a workplace group or individually (this is part of the legitimate interest of the SCoR)
- For elections and appointments to committees (this is part of the legitimate interest of the SCoR)
- To invite people to participate in surveys and research (this is part of the legitimate interest of the SCoR)
- To deliver Continuous Professional Development (this is part of the legitimate interest of the SCoR)
- For nominations and awards (this is part of the legitimate interest of the SCoR)
- To assist with personal injury claims (we get active consent from members for this)
- To process benevolent fund applications (we get active consent from members for this)
- To undertake equal opportunities monitoring.

We also keep information about our employees, present, past and prospective. This is used for recruitment, employment, payroll and monitoring purposes.

Sharing personal information

We never sell personal information. We never share it with organisations outside of SCoR for their own use unless we have prior consent to do so or are required to do so by law.

Where we need to use third party organisations to process personal information on our behalf, for example a mailing house, we put in place a contract with the company to ensure that the personal information that we provide to them is properly protected and handled.

If we transfer personal information to countries or jurisdictions which may not provide the same level of data protection as the UK, we will put in place a contract with the company that we transfer the information to in order to ensure that the data is properly protected.

Data subject rights

Subject access

People have a right to access most information an organisation holds about them. We will provide information if asked. This is known as a Subject Access Request (SAR). We have a

DATA PROTECTION COMPLIANCE HANDBOOK

procedure which is managed by the SCoR Data Protection Officer. We have very limited time to respond to a SAR so it is important that you report any requests to the Data Protection Officer immediately. You can review the SAR procedure [here](#).

Direct marketing communications

People have a right to not receive communications from which promote SCoR campaigns, aims and objectives. We send SCoR email newsletters and magazines such as Synergy News to our members as a member benefit. However, members have the right to unsubscribe from receiving these.

To be informed

People have a right to be informed about why and how we collect, store, use and share their personal information. The SCoR Data Protection Officer maintains a record of this in the privacy policy which is available on the SCoR website. Please contact the Data Protection Officer immediately if a member asks you for the detail of how their personal information is used and you are uncertain how to respond.

Data erasure

People have a right to request that their personal information is deleted when there is no compelling reason for it to be retained by us. This right may override the SCoR retention policy and schedule. Please inform the SCoR Data Protection Officer immediately if you receive a request to delete someone's personal information. We may need to retain some of the personal information.

The aim of the General Data Protection Regulation is to protect the rights of individual data subjects; it is everybody's responsibility to ensure that SCoR always fully complies with the Act.

I have read and understood SCoR's data protection policies referenced in the attachment to this declaration.

I understand that I am only to use or process personal data to which I am given access by SCoR for the purpose authorised by SCoR and in accordance with SCoR's data protection privacy policy.

I understand I must keep personal and sensitive personal data secure and in particular will not make any unauthorised disclosure of personal data to any third party.

DATA PROTECTION COMPLIANCE HANDBOOK

Our data protection operating procedures

A good way of thinking about data protection compliance is to treat people's personal information as you would expect your own information to be treated. In particular you must:

1. Be open and clear with people about how their personal information will be used by the SCoR.
2. Tell members when collecting their personal information or if asked, what you intend to do with it.
3. Include a privacy notice explaining what SCoR uses personal information for in paper and electronic forms when collecting personal information, for example in the membership form.
4. Speak to the SCoR Data Protection Officer if you are designing a new form which will be used to collect personal information, so that s/he can ensure an appropriate privacy notice is included.
5. Check that we have the consent of a member (and it is recorded) before sharing any of their information with an organisation or person outside of the SCoR.
6. Only ever use personal information for the purpose for which a member originally provided their information.
7. Keep only personal information that the SCoR actually needs - even if someone voluntarily gives you more information than you ask them for.
8. Remember that any information that you record about a member, electronically or on paper, could be provided to the member as part of a subject access request.
9. Encourage members to inform us if their personal information changes or they believe any of our information is inaccurate.
10. Update our records promptly to ensure that the personal information we hold and use is accurate.
11. Inform your manager of any changes to your own personal information.
12. Follow the SCoR retention schedule which states how long certain types of personal information should be kept for before being archived or destroyed securely. You can view the [SCoR retention here](#).
13. Regularly review the records you are responsible for to ensure that you are complying with the SCoR retention schedule.
14. Use confidential waste or a shredder when disposing of personal information which is no longer needed.

DATA PROTECTION COMPLIANCE HANDBOOK

15. Forward the contact details of anyone who asks to see the information that we hold about them to the SCoR [Data Protection Officer](#) immediately.
16. Report requests for erasure or deletion of personal information to the SCoR Data Protection Officer.
17. Treat personal information as confidential at all times.
18. Take care to ensure that you do not accidentally disclose personal information to other people, particularly when working away from the office, at home, at other locations or while travelling.
19. Ensure other people do not have access to your computer and manual records which contain personal information.
20. Switch off your computer or use a password protected screen saver when you leave your screen unattended.
21. Protect your computer and mobile devices which are used to access personal information, with passwords, and keep your passwords secret.
22. Keep your desk clear of personal information.
23. Keep hard copy records of personal information locked away in a drawer or cabinet.
24. Use recorded delivery or a courier if you have to post paper records containing personal information.
25. Password-protect and encrypt files containing personal data of more than 10 individuals before emailing them.
26. Use secure file transfer service to transfer large volumes of personal information and sensitive personal data outside of the SCoR – speak to IT for help with this.
27. Ensure that your old equipment such as a redundant laptop is “cleaned” before being disposed of.
28. Ensure no one can read SCoR personal information recorded on paper, your laptop, tablet or mobile phone when you are working and travelling by public transport.
29. Obtain approval from the Data Protection Officer if you need to and before you send any personal information outside the European Economic Area.

Personal Data Breaches

If you think that you might have inadvertently breached the data protection legislation in any way at all, for example, by losing personal information or accidentally disclosing it, contact the SCoR Data Protection Officer at dpo@sor.org immediately. We have a [procedure](#) for assessing and reporting any personal data breaches to ensure that we respond properly and promptly.

DATA PROTECTION COMPLIANCE HANDBOOK

Responsibility Agreement

[Please fill out the agreement online](#)