Office of the Scottish Charity Regulator

Data Protection Policy

Contents

Introduction

The Scottish Charity Regulator (OSCR) and its employees are bound by a legal duty of confidentiality to all data subjects which can only be set aside to meet an overriding public interest, legal obligation, or similar duty.

The Data Protection Act (DPA) 1998 imposed obligations on the use of all personal data held by OSCR, whether it relates to data subjects and their families, employees, complainants, contractors or any other individual who comes into contact with the OSCR. This has implications for every part of OSCR.

The introduction of the EU Directive - General Data Protection Regulations (GDPR) and the enabling Data Protection Act introduces some changes to Data Protection

OSCR is a Data Controller, as defined in Section 1 of the DPA, and is obliged to ensure that all of the DPA requirements are implemented. The DPA applies to all staff, contractors and volunteers.

This policy sets out how OSCR meets its legal obligations and requirements under the Act. It will be reviewed annually, or as appropriate to take into account changes to legislation that may occur, and/or guidance from the Government and/or the Information Commissioner.

Requirements of Legislation

The Data Protection Act 2018 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

Management and Responsibilities

The Chief Executive, as Accountable Officer (AO), has overall responsibility for data protection within OSCR. The Head of Support Services is designated as OSCR's Senior Information Risk Owner (SIRO). The implementation of, and compliance with, this policy is delegated to the Data Protection Officer (DPO). The DPO for OSCR is the Information Manager (IM).

All managers are responsible for ensuring that this policy is communicated and implemented within their area of responsibility. They are responsible for the quality, security and management of personal data in use in their area. Advice and guidance regarding this policy or the DPA in general is available here or from the Support Services Team.

All data protection and information security related incidents must be reported immediately on being discovered to the DPO and properly investigated according to OSCR's Information Security Policy. In the main, correspondence with the Information Commissioner's Office (ICO) on data protection matters will be dealt with by the DPO.

The Data Protection Principles

The Data Protection Act 2018 is underpinned by 6 principles. The principles apply to all personal data, irrespective of how it has been obtained, and if you make sure you handle personal data in line with these principles then compliance with the DPA is likely.

Principle 1 - Processing of personal data shall be lawful, fair and transparent.

Conditions for Processing

"Processing" broadly means any operation(s) which is performed on personal data or sets of personal data, whether automated or not such as collecting, recording, organisation, structuring, adapting or altering, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making it available, retaining or disposing of personal data, and if any aspect of processing is unfair, there will be a breach of the first data protection principle. Before we can process any individual's personal data we must ensure that the "conditions for processing" are met. The conditions for processing are stated the Data Protection Act. The conditions for processing are more exacting when sensitive personal data is involved, such as information about an individual's health or criminal record.

Privacy Notices

When personal information is collected about individuals, they should be told exactly how that information is to be used. This is called a "privacy notice". This should tell them

- your identity (business area);
- the reasons (purpose(s)) you intend to process the information; and
- anything extra you need to tell individuals in the circumstances to enable you to process the information fairly.

If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether or not to enter into the relationship.

Disclosure of personal information

Information about identifiable individuals should only be disclosed on a need to know basis. Disclosures of information may occur because of a legal requirement eg with a Court Order. Specific legislation covers some disclosure (eg for tax and pension purposes). The validity of all requests for disclosure of personal data without consent from the individual must be checked. The identity of those requesting data and their legal right to request or demand information must be validated. The reasons for disclosures made without consent must be documented.

Police officers or others requesting information for the purposes of a criminal investigation, including for benefit, tax or immigration offences, should be asked to put their request in writing, either by using a standard data protection request form, or by letter / email. This requirement can be set aside where the request is made in an emergency (i.e. a person is in immediate and imminent risk of serious harm).

The request should include:

- What information is needed
- Why it is needed
- How the investigation will be prejudiced without it

Principle 2 - Personal data shall be collected only for one or more specified, explicit and legitimate purposes, and shall not be processed in any manner incompatible with the purpose(s) for which it is collected;-

a) unless the controller is authorised by law to process the data for that purpose, and
b) the processing is necessary and proportionate to that other purpose.

Notification

OSCR must provide an annual notification to the Information Commissioner, summarising the purposes for the use of personal data by OSCR. Failure to submit the annual notification or to keep it up to date is a criminal offence.

The DPO is responsible for submitting the notification. All managers should inform the DPO if their areas of responsibility change or develop in such a way that they will begin to process personal data or they will process it in a substantially different way. This will allow the DPO to make any necessary changes to OSCR's notification.

Incompatible re-use of information

Personal data must not be re-used for any purpose that is incompatible with the original purpose it was collected.

Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

Managers should ensure that any data collected from individuals is complete but not excessive, and the level of data retained on OSCR systems should be appropriate for current, existing purposes.

Principle 4 - Personal data undergoing processing must be accurate and, where necessary, kept up to date.

Information Asset Owners and team managers must ensure that personal data they are responsible for and stored in any way on any media is accurate and kept up to date.

The accuracy of Staff information should also be checked on a regular basis – either by line managers or by HR.

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes for which it is processed.

Personal data must not be retained indefinitely, and managers must ensure that they are aware of, and compliant with, OSCR's Information Management policy and principles including the agreed retention schedules for all documents and files.

Principle 6 - Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

Security

All information relating to identifiable individuals must be kept secure at all times. Managers must take steps to ensure that office environments and working practices take account of the security necessary to prevent the loss, theft, damage or unauthorised access to personal information. Information Asset Owners (IAOs) are responsible for ensuring that all systems storing personal data, or other assets or repositories of information are appropriately risk-assessed and protected from identifiable threats.

Advice on securing information can be found in the IT Code of Conduct and the Information Security Summary.

Data Processors

Where OSCR uses a contractor to process personal data on its behalf, the contractor must sign a data processing agreement which ensures that they are taking adequate steps to comply with Principle 6 (and all other DPA requirements) on OSCR's behalf. OSCR retains legal responsibility for the actions of processors, and so those managing contracts must ensure that all security procedures necessary are specified in the contract, and it is subsequently monitored to ensure that they are in place. Further advice can be obtained via Support Services.

Reporting of Incidents

In the event of any loss or theft of data, (either by loss of a portable device or other media such as an Ironkey) or suspected cyber attack where there is a loss of data, OSCR must report this to the Information Commissioner. It is imperative that staff report any loss or theft to the Data Protection Officer or Support Services as soon as they become aware of the incident. We are legally obliged to report any loss or data breach within 72 hours of discovery, failure to report could result in a civil penalty.

The Right to Information

Individuals have a number of rights, including: access to their personal information (subject access request); preventing or stopping processing likely to cause substantial harm or distress; preventing or stopping direct marketing; the right to take action for compensation for breaches of the DPA which cause damage; and a right to rectify, block, erase or destroy inaccurate data.

Subject Access

Individuals have a right to request any personal data held by OSCR in whatever form. OSCR has a procedure to deal with requests for access to information (known as Subject Access Requests (SARs)) – all SARs must be sent to Support Services. The Team will then advise on how to proceed.

Transfer of Data outside of the European Union or EEA

Any manager who is required to send personal identifiable information in any format to countries outside the EEA, must discuss this with Support Services as the levels of protection for the information may not be as comprehensive as those in the UK.

Staff Awareness

Training

All staff must be trained before they can handle personal information in any form in the course of their job.

Scottish Government and OSCR have a mandatory training programme which includes maintaining awareness of data protection and information handling for all staff. This is carried out by annual completion of e-learning as follows:

- Data Protection e-learning package;
- Responsible for Information e-learning package.

Disciplinary issues

A deliberate or reckless breach of the DPA could result in a member of staff facing disciplinary action. Managers must ensure that all staff familiarise themselves with the content of this policy.

All personal data recorded in any format must be handled securely and appropriately in line with the DPA, and staff must not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff will be considered as a disciplinary issue. Employees should be aware that it is a criminal offence to deliberately or recklessly disclose personal data without the authority of OSCR (the data controller).