Data Protection Policy

Document Properties

Change Record

Version	Revision	Author	Description	Date
0	1	R Jackson	Initial Draft	07//02/2018
0	2	C James	Reviewed and minor amends	07/05/2018
0	3	C James	Incorporated comments from S Davenport	22/05/2018
0	4	C James	Further minor amends to 7.4 and 9.1	25/05/2018

Document Approval

Approving Body or Person	Role (review, approve)	Date
Statutory Officers' Group	Approve	

1. Introduction

1.1 Sheffield City Region (SCR) is fully committed to compliance with the requirements of the General Data Protection Regulation (Regulation EU 2016/679) (GDPR) which came into force on 25th May 2018. SCR will therefore instigate and apply procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners, or other servants of the organisation who have access to any personal data held by or on behalf of SCR are fully aware of and abide by their duties and responsibilities under the GDPR.

1.2 Under the GDPR, both Data Controllers and Data Processors are liable for data breaches. SCR is classed as a Data Controller and could be prosecuted for any serious breaches of the GDPR that may be committed.

2. Policy Statement

2.1 In order to operate efficiently, SCR collects and uses information about people with whom it communicates. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, SCR may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used. Personal information may be recorded on paper, in computer records or other formats which must all comply with the principles of the GDPR.

2.2 In carrying out our responsibilities we have cause to collect and use information about individuals for whom we provide services. We may also use the information to derive statistics to provide informed decisions, but use them in such a way that individuals cannot be identified from them.

2.3 SCR regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the organisation and those with whom it carries out business. SCR will ensure that it treats personal information lawfully and correctly.

Where applicable, SCR will ensure that it takes measures that meet the principles of data protection by design and data protection by default. These may include:

- data minimisation;
- pseudonymisation;
- transparency;
- allowing individuals to monitor processing; and
- creating and improving security features on an ongoing basis.

2.4 To this end, SCR fully endorses and will adhere to the principles of data protection as set out in the GDPR. GDPR compliance will be achieved through a combination of processes, actions and procedures that will be monitored for their consistency and effectiveness to support the detailed principles contained within this policy.

3. Scope

3.1 This policy informs staff, members of the public and external parties of the processes SCR has established for complying with the GDPR.

3.2 This policy operationally applies to all employees of the organisation, elected members, contractors, agents, partners and temporary staff working for or on behalf of SCR.

3.3 The GDPR does not apply to requests for information about a person if they are deceased. These requests should be processed in accordance with the Freedom of Information Act (FoIA) 2000, but should also be considered fairly and lawfully.

4. GDPR Principles

4.1 Under Article 5 of the GDPR, the data protection principles set out the main responsibilities for organisations. SCR will comply with these principles. The principles require that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

5. Conditions for Processing

5.1 The GDPR provides conditions for the processing of any personal data. It also makes a distinction between "personal data" and "sensitive personal data". Sensitive personal data requires stricter conditions of processing.

5.2 "Personal data" is defined as any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

5.3 The GDPR requires organisations to determine their lawful basis for processing each category of personal data they hold before they process it.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever SCR processes personal data:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The SCR Privacy Notice on the website describes the lawful bases for processing.

5.4 The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Extra conditions must be satisfied before this data can be processed lawfully.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

6. Individuals' Rights

6.1 Depending on which lawful basis for processing applies, individuals have the following rights.

Where relevant, SCR will ensure that individuals are given these rights as defined within the GDPR including:

a) The right to be informed - The right to be informed encompasses the obligation to provide 'fair processing information', typically through a privacy notice. SCR's privacy notice is published on its website.

b) The right of access - Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Information must be provided free of cost and at the latest within one month of the receipt of the request. SCR's has established a process for dealing with Subject Access Requests, which is set out in SCR's Guide to FOI, Subject Access and Environmental Information Requests Procedure.

c) The right to rectification - The GDPR gives individuals the right to have personal data rectified. SCR will allow individuals to request rectification of their personal data if it is

inaccurate or incomplete. SCR will do this within one month of receiving the request for rectification.

d) The right to erasure – The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. SCR will delete an individual's data where it receives a request for erasure subject to the exceptions outlined in the GDPR.

e) The right to restrict processing - Individuals have a right to 'block' or suppress processing of personal data in certain circumstances. When processing is restricted, an organisation is permitted to store the personal data, but not further process it. It is possible to retain just enough information about the individual to ensure that the restriction is respected in future. SCR will ensure that it complies with this right.

f) The right to data portability - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services in specific circumstances. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. SCR will do this within one month of receiving the request.

g) The right to object - Individuals have the right to object to right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics. Unless there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or unless the processing is for the establishment, exercise or defence of legal claims, SCR will stop processing the personal data.

h) Rights in relation to automated decision making and profiling – The GDPR requires organisations to give individuals information about any automated decision making and processing. SCR does not use any automated decision-making systems at present.

7. Roles and Responsibilities

7.1 All individuals permitted to access personal data on behalf of SCR must agree to comply with this Policy and will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

Any breach of any provision of the GDPR will be deemed as being a breach of any contract between SCR and that individual, company, partner or firm.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to disciplinary procedures, including dismissal where appropriate, and possible legal action.

7.2 Managers are required to ensure that the service areas for which they are responsible have in place adequate guidance on data protection and effective measures to comply with this policy.

7.3 Third parties who are users of personal information supplied by SCR will be required to confirm that they will abide by the requirements of the GDPR with regard to information

supplied by SCR and allow data protection audits by SCR of data held on its behalf (if requested); and

Indemnify SCR against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

The GDPR does not give third parties rights of access to personal information for research purposes, unless a contractual agreement has been established between SCR and the third party to perform research services.

7.4 SCR will ensure that:

- Everyone managing and handling personal information understands that they are responsible for following good data protection practice;
- Staff who handle personal information are appropriately supervised and trained;
- Privacy by design measures are implemented when processing Personal Data and that staff will complete privacy impact assessments where necessary.
- Queries about handling personal information are promptly dealt with;
- People know how to access their own personal information;
- Methods of handling personal information are regularly assessed and evaluated;
- Any disclosure of personal data will be in compliance with approved procedures;
- All necessary steps will be taken to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure; and
- All contractors who are users of personal information supplied by SCR will be required to confirm that they will comply with the requirements of the Regulation with regard to information supplied by SCR.
- Data breaches are reported to the Information Commissioner's Officer within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, SCR will also inform those individuals without undue delay. SCR have put in place procedures to deal with any suspected Personal Data Breach;
- A DPO is in post. The DPO's role is to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; training staff and conducting internal audits;
- Any data transferred outside the EEA meets the conditions required by GDPR;
- Full and accurate records of data processing activities;
- Personal Data will not be shared with third parties unless appropriate safeguards and contractual arrangements are in place;
- Automated decision making does not take place without the consent of the DPO;
- Rules regarding direct marketing are observed.

8. Information Commissioner - Notification and Registration

8.1 SCR has registered its use of personal data with the Information Commissioner and the register references are given below. The registers can be accessed and searched on the Information Commissioner's website: http://www.ico.org.uk.

Data Controller: Sheffield City Region Combined Authority
Registration Ref: ZA092329

SCR will review the Data Protection Register annually and notify the Information Commissioner of any amendments.

9. Complaints

9.1 SCR has a complaints procedure and any complaints about the Data Protection Act, the Environmental Information Regulations or the Freedom of Information Act may be dealt with by clearly marking your correspondence 'Complaint' and addressing it to:

Data Protection Officer
Broad Street West
Sheffield
S1 2BQ
DPO@sypte.co.uk

9.2 If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:

Customer Services Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9
5AF

Web: http://www.ico.org.uk
Tel: 01625 545 745

10. References and Related Documents

10.1 References

- General Data Protection Regulation (Regulation EU 2016/679)
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990

10.2 Related documents

- Privacy notice guidance
- Subject Access Request guidance
- Information Sharing guidance (currently under review)
- Information Classification and Data Handling guidance (currently under review)
- Data Quality policy and related guidance
- Records Management policy and related guidance
- Information Security policy and related guidance
- Freedom of Information policy and related guidance