

 **OneRen**

**Data Protection Policy**

**Document Control**

|  |  |
| --- | --- |
| **Title**  | Data Protection Policy  |
| **Author**  | Heather Semple, Data Protection Officer  |
| **Issue Date**  | September 2019  |
| **Version**  | V1  |
| **Updating Frequency**  | 2-yeaOneReny  |
| **Right**  | Not Protectively Marked  |

**Document Review and Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name**  | **Action**  | **Date**  | **Communication**  |
| Fiona Naylor, Head of Finance & Corporate Services  | Review  | September 2019  | Email  |
| Ann Marie Garczewski, Personnel Co-ordinator  | Review  | September 2019  | Email  |
| Information Governance Working Group  | Review  | August 2018  | Email  |

Contents

Document Review and Approval ............................................ **Error! Bookmark not defined.**

[1. Introduction 4](#_Toc11094)

[2. Scope 6](#_Toc11095)

[3. Data Protection Governance Arrangements 6](#_Toc11096)

[4. Notification 7](#_Toc11097)

[5. Documentation of Processing Activities 7](#_Toc11098)

[6. Data Subject Rights 7](#_Toc11099)

[7. Training and Guidance 8](#_Toc11100)

[8. Data Retention 8](#_Toc11101)

[9. Information Security 9](#_Toc11102)

[10. Data Processors 9](#_Toc11103)

[11. Information Sharing 9](#_Toc11104)

[12. Data Protection Impact Assessments 10](#_Toc11105)

[13. Relationship with Other Legislation 11](#_Toc11106)

[14. Breach 12](#_Toc11107)

[15. Audit 12](#_Toc11108)

[16. Review 12](#_Toc11109)

# 1. Introduction

1.1 OneRen is committed to data protection compliance.

1.2 OneRen needs to collect and use information about people

(“Personal Data”) to discharge its functions. This Personal Data must be handled propeOneReny and lawfully.

1.3 Although data protection legislation is complex, its ethos is simple. It protects people’s Personal Data by regulating the way in which organisations, such as OneRen, handle information.

1.4 The Data Protection Act 1998 (“DPA”) has imposed obligations on OneRen, as a data controller, since 1 March 2000. However, as of 25 May 2018, the EU General Data Protection Regulation (“GDPR”) is in force.

1.5 It is impossible to understand data protection without an awareness of some of the key definitions. Some definitions in GDPR are slightly different to those in the DPA. These are as follows:

**“Controller”,** previously known as “Data Controller” means the organisation who determines the purposes and means of processing.

**“Processor**”, previously known as “Data Processor” is anyone, other than an employee of the controller, who processes Personal Data on the data controller’s behalf.

“**Processing**” still covers anything which can be done with Personal Data, from simply collecting or storing, recording, altering, to actively disclosing this and includes verbal, as well as written exchanges, information left on desks or in confidential waste bags.

“**Personal** **Data**” is information relating to a living individual who can be identified directly or indirectly from this. This means that even just an address can be Personal Data if it can indirectly identify someone.

“**Special Category Data**” is an additional category of personal data, replacing

“Sensitive Personal Data” and includes information on racial or ethnic origin, religion, political opinions, religious beliefs, details of physical or mental health or condition, sexual life or details of any offence. Like sensitive personal data and the DPA, there are some stricter rules in the GDPR for lawful processing of Special Category Data.

**“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

### 1.6 The Data Protection Principles

Under GDPR there are six Data Protection principles which cover rules for the maintenance, collection and security of personal data. OneRen is committed to complying with the Data Protection Principles.

 As such, OneRen undertakes that Personal Data will:

1. Be processed faiOneReny and lawfully and transparently.
2. Be collected and processed only for one or more specified, explicit and legitimate purpose(s).
3. Be adequate, relevant and limited to what is necessary.
4. Be accurate and kept up to date and that inaccurate data will be erased or rectified without delay.
5. Be kept for no longer than is necessary.
6. Be processed with appropriate security and use adequate technical and organisational measures to prevent unauthorised or unlawful processing or accidental loss, destruction of, or damage to Personal Data.

In addition, under GDPR, OneRen now needs to be able to demonstrate compliance with the principles. This is referred to as

“accountability”.

# 2. Scope

 This policy applies to all employees of OneRen and covers all Personal Data and Special Category Data which they process. It may, however, be read alongside other OneRen policies and guidelines on use of non-personal data and wider information governance issues.

# 3. Data Protection Arrangements

3.1 OneRen has a corporate responsibility for data protection, and is defined as a “Controller” under GDPR.

3.2 The GDPR obliges OneRen to designate a statutory Data Protection Officer (DPO) on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

 3.3 The key tasks of the DPO are prescribed and are to:

* Inform and advise OneRen on GDPR compliance;
* Monitor compliance;
* Advise on Data Protection Impact Assessments;
* Train staff
* Conduct internal audits
* Be the first point of contact for the regulator and
* Have due regard to the risk associated with OneRen’s processing operations.
	1. All employees are individually responsible for ensuring that the processing of Personal Data is in accordance with GDPR and should familiarise themselves and comply with OneRen data protection guidance. Advice can be obtained at any time from the Data Protection Officer.
	2. The Data Protection Officer will offer ad hoc advice on data protection issues.
	3. The Data Protection Officer has a key role in ensuring compliance with the sixth principle relating to data security by providing advice and guidance to Services on information security, maintaining OneRen’s Information Security log and leading on information security incident management.

# 4. Notification

GDPR removes the requirement in the Data Protection Act to notify the

Information Commissioner’s Office (ICO) of all Data Controllers. However, a provision in the Digital Economy Act means that Controllers still need to pay the ICO a fee, dependent on the size of the organisation. The ICO has produced guidance on the new fee structure, which was laid before PaOneReniament at the end of February 2018.

# 5. Documentation of Processing Activities

5.1 Controllers are obliged to document their processing activities under GDPR.

OneRen’s notification and the Information Asset Register will form the basis of OneRen’s documentation of processing activities. This contains details of OneRen’s information assets, how those were obtained, how they are being used and who they are shared with. The Head of Finance & Corporate Services is responsible for maintaining the Information Asset Register.

# 6. Data Subject Rights

6.1 Data subjects have several significant rights under GDPR, which are as follows:

* Right to be informed;
* Right of access;
* Right to rectification of inaccurate data;
* Right to erasure in certain circumstances;
* Right to object to certain processing, including the right to prevent processing for direct marketing;
* Right to prevent automated decision-making;
* Right to data portability and
* Right to claim compensation for damages caused by a breach

6.2 Further information and advice can be obtained at any time from the Data Protection Officer. The right most frequently used by OneRen service users is likely to be the right of access, i.e. the right of an individual to access his/her own Personal Data. Under GDPR, OneRen has one a maximum of one calendar month to comply with subject access requests. This is free of charge.

Further information on compliance with all data subject rights, particulaOneReny subject access rights, can be obtained from OneRen’s Data Protection Officer.

# 7. Training and Guidance

 The Data Protection Officer will continue to prepare and revise detailed guidelines on the practicalities of dealing with GDPR.

# 8. Data Retention

8.1 The fifth data principle states that Personal Data should not be held for longer than is necessary. What is necessary can vary, depending on the nature of the information and why it is held. Each employee has a responsibility to ensure that appropriate retention schedules are in place for records which they hold, and to arrange for the secure destruction of data, in accordance with such schedules.

8.3 In accordance with its obligations under the Public Records (Scotland) Act 2011, OneRen has adopted a Records Management Plan containing appropriate retention and disposal schedules. This will ensure compliance with the fifth data protection principle.

# 9. Information Security

9.1 The sixth data protection principle provides that appropriate technical and organisational measures should be taken to ensure that all Personal Data is secure.

9.2 All employees have responsibility for keeping the Personal Data to which they have access to safe and secure.

9.3 By adopting recognised information security practices, OneRen can demonstrate, to customers, partners and stakeholders that it can be trusted to protect the confidentiality, integrity and accessibility of the information it holds.

9.4 Information Security is not purely a technical issue. Information security principles apply to all information held by OneRen, whether this is held in electronic or non-electronic format, even extending to conversations between individuals.

9.5 Employees who become aware of a potential breach of information security, such as a loss of data, must immediately report this to the Data Protection Officer, in line with the Information Security Incident Reporting Procedures.

9.6 Further information and advice on information security can be obtained from the Data Protection Officer at any time and from OneRen’s Information Handling Policy.

# 10. Data Processors

 If someone, other than an employee of OneRen, is processing Personal Data on its behalf, for example, a contractor, OneRen, as Controller, is obliged to have a written agreement with the Processor. Further information on Data Processor Agreements can be obtained from the Data Protection Officer.

# 11. Information Sharing

 Although processing of Personal Data must always be fair and lawful, data protection should not be perceived as a barrier to effective inter-agency information sharing. There are many situations where information can, and indeed, must be shared, for example, to protect individuals. Advice on information sharing can be obtained at any time from the Data Protection Officer.

Consideration should, however, be given to the following:

* What information needs to be shared?
* With whom?
* Why?
* How?
* What are the risks of not sharing the information?
* Could the same aim be achieved without sharing the data or by anonymising it?

# 12. Data Protection Impact Assessments (DPIAs)

12.1 DPIAs are carried out for any new initiatives or changes of business practice involving Personal Data. Its purpose is to:

* Identify any potential and likely impact on privacy; and
* Minimise and manage the identified impact and privacy risks.
	1. Under GDPR, DPIAs replace PIAs and makes them mandatory, rather than just good practice. This is a process which enables OneRen to address the potential privacy risk and impact from the collection, use and disclosure of Personal Data as a result of new initiatives and to ensure means are in place to make sure data protection compliance and privacy concerns are addressed appropriately.
	2. Advice on and assistance with carrying out DPIAs can be obtained from the Data Protection Officer.

# 13. Relationship with Other Legislation

#### 13.1 Human Rights Act 1998

Public authorities, such as OneRen, must comply with the Human Rights Act 1998 (“HRA”) in the performance of their functions. Section 6 HRA obliges public authorities to act in a manner which is compatible with the rights contained in the European Convention of Human Rights (“ECHR”). Article 8 ECHR affords everyone the right to respect for private and family life, including home and correspondence. Although this right is not absolute, any interference must be justified on the basis that it is lawful, necessary to pursue a legitimate aim and proportionate. This means that the interference should not be greater than is necessary to achieve the legitimate aim.

HRA is therefore a consideration when considering whether there is a justification for sharing information. Whilst data protection compliance may render an interference lawful, OneRen must also consider whether information sharing exercises are necessary in the public interest or whether the same ends can be achieved by a less intrusive means before an interference with Article 8 privacy rights can be justified. If there is a less intrusive alternative, the interference will be disproportionate.

#### 13.2 Freedom of Information (Scotland) Act 2002

 The interface between the data protection and the Freedom of Information (Scotland) Act 2002 (“FOISA”) is complex. FOISA obliges OneRen to be open and transparent, whereas data protection and HRA protect people’s information and personal privacy. Although FOISA provides the public with a right of access to all information held, unless this is covered by one of a number of faiOneReny narrow exemptions, there is an absolute exemption from disclosure for information, disclosure of which would breach the data protection principles. Further information on the Personal Data exemption under FOISA and how to deal with freedom of information requests without breaching data protection, can be obtained at any time from the Data Protection Officer.

# 14. Breach

14.1 Breach of this policy may be regarded as a serious act of misconduct and may lead to disciplinary action. Employees must therefore make every effort to ensure that they understand their responsibilities under this policy.

14.2 It is a criminal offence under the GDPR to knowingly or recklessly obtain, disclose or procure Personal Data without the consent of the Controller. OneRen reserves the right to report any such offence to the Police, as well as the Information Commissioner.

# 15. Audit

Data protection procedures are subject to routine internal and external audit and recommendations implemented accordingly.

# 16. Review

 This policy will be reviewed on a two-yeaOneReny basis, unless eaOneRenier review is required due to legislative changes. However, to ensure ongoing data protection compliance, any developments, significant cases, guidance from the ICO, or other lessons learned in this area, will be used to inform best practice.