



Onix DC - ISMS-A.1801

Legal Responsibilities Policy

Document History

Prepared By	Version	Date	Signature	Comment
Michael Offei Thompson	1.0	02.11.2022	M. O. T	

Document Approval / Review

	Name	Designation	Signature	Date
Prepared				
Reviewed				
Approved	Michael Offei Thompson	Chief Executive Officer		16.11.2022

Distribution

Name	Date
All staff of Onix DC	16.11.2022
All Interested Parties	16.11.2022

Contents

1	INTRODUCTION.....	5
1.1	RISKS ADDRESSED	ERROR! BOOKMARK NOT DEFINED.
1.2	SCOPE	5
1.3	RELATED DOCUMENTS.....	ERROR! BOOKMARK NOT DEFINED.
1.4	PURPOSE	5
2	RELEVANT LEGISLATION.....	6
2.1	INTELLECTUAL PROPERTY RIGHTS.....	ERROR! BOOKMARK NOT DEFINED.
2.2	PROTECTION OF ORGANIZATIONAL RECORDS	6
2.3	DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION.....	6
2.4	PREVENTION OF MISUSE OF INFORMATION PROCESSING FACILITIES	7
2.5	REGULATION OF CRYPTOGRAPHIC CONTROLS	ERROR! BOOKMARK NOT DEFINED.
3	THE DATA PROTECTION ACT.....	8
3.1	DEFINITIONS	8
3.2	THE EIGHT PRINCIPLES OF DATA PROTECTION	8
3.3	RIGHTS OF THE INDIVIDUAL.....	9
3.4	ADDRESSING COMPLIANCE TO THE DATA PROTECTION ACT	9

1 Introduction

1.1 Scope

This control applies to all systems, people and processes that constitute Onix DC's information systems, including board members, directors, employees, suppliers and other third parties who have access to Onix DC systems.

1.2 Purpose

In its everyday business operations, Onix DC makes use of a variety of data about companies and individuals, such as:

- Current, past, and prospective employees
- Suppliers
- Customers
- Other stakeholders

In collecting and using this data, Onix DC is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Onix DC is taking to ensure that it complies with it.

2 Relevant Legislation

In the context of its business operations and the industry in which it operates, the following major pieces of legislation are relevant to Onix DC.

This list will be revised as further legislation comes into force.

The remainder of this policy document deals with the provisions of the first of the legislative items on the above list in further detail – the Data Protection Act.

2.1 Protection of Organizational Records

Legislation	Areas Covered
The Data Protection Act 2012	Collection, use and disposal of personal information

2.2 Data Protection and Privacy of Personal Information

Legislation	Areas Covered
The Data Protection Act 2012	Collection, use and disposal of personal information

2.3 Prevention of Misuse of Information Processing Facilities

Legislation	Areas Covered
Cybersecurity-Act-2020-Act-1038	Unauthorized access to systems and networks
The Regulation of Investigatory Powers Act 2000	Hidden surveillance of staff

3 The Data Protection Act

The Data Protection Act is one of the most significant pieces of legislation affecting the way that Onix DC carries out its activities. Significant fines are now applicable if a breach is deemed to have occurred under the Act, which is designed to protect personal data.

3.1 Definitions

Personal data is defined as:

“data which relate to a living individual who can be identified:

- a) from those data; or
- b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller;

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Sensitive personal data is defined as:

“Personal data consisting of information as to:

- a) the racial or ethnic origin of the data subject,
- b) his political opinions,
- c) his religious beliefs or other beliefs of a similar nature,
- d) whether he is a member of a trade union,
- e) his physical or mental health or condition,
- f) his sexual life,
- g) the commission or alleged commission by him of any offence, or
- h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

3.2 The Eight Principles of Data Protection

The Data Protection Act 2012 sets out principles of good practice all of which are legally enforceable.

The principles require that personal information:

1. Shall be processed fairly and lawfully and, shall not be processed unless specific conditions are met

2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed
4. Shall be accurate and where necessary, kept up to date
5. Shall not be kept for longer than is necessary for that purpose or those purposes
6. Shall be processed in accordance with the rights of data subjects under the Data Protection Act 2012
7. Shall be kept secure - i.e., protected by an appropriate degree of security
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection

3.3 Rights of the Individual

The data subject also has rights under the Data Protection Act. These consist of:

- The right to be informed that processing is being undertaken
- The right of access to one's personal information within the statutory 40 days
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block, or erase information regarded as wrong information

3.4 Addressing Compliance to the Data Protection Act

The following actions are undertaken to ensure that Onix DC always complies with the provisions of the Data Protection Act:

- All staff involved in handling personal information understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Routes are available to members of the public wishing to enquire about our handling of personal information and such enquiries are handled effectively
- Regular reviews of procedures involving personal information are carried out