

Appendix 2: Statutory Requirements Summary

Data Protection Act 2018

<http://www.legislation.gov.uk/ukpga/2018/12/contents>

The Data Protection Act regulates the use of personal data by organisations. Personal data is defined as information relating to a living, identifiable individual.

The Act is underpinned by six guiding principles which requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- 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 ('purpose limitation');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 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 ('accuracy');
- 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 ('storage limitation');
- 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 ('integrity and confidentiality')."

As a data controller, the City Corporation must also notify annually with the Information Commissioner's Office. The Act also places a responsibility on the Controller to notify the ICO of data breaches within 72 hours. The Information Commissioner has the power to issue fines of up to 4% of annual global turnover or 20 million euros (whichever is the greater) for a breach of the Data Protection Act.

Freedom of Information Act 2000

<http://www.legislation.gov.uk/ukpga/2000/36/contents>

The Freedom of Information Act gives individuals a right of access to information held by the City Corporation, subject to a number of exemptions. Requests for information must be made in writing (email, letter or fax) but can be received by any member of staff at the City Corporation. Such requests must be responded to within 20 working days. The City Corporation has an internal appeal process if a requester is unhappy with a response to a request and the Information Commissioner regulates the Act.

Privacy and Electronic Communications Regulations 2003

<http://www.legislation.gov.uk/uksi/2003/2426/contents/made>

Section 11 of the Data Protection Act allows individuals to control the direct marketing information they receive from organisations. The Privacy and Electronic Communications Regulations specifically regulate the use of electronic communications (email, SMS text, cold calls) as a form of marketing and allow individuals to prevent further contact.

Regulation of Investigatory Powers Act (RIPA) 2000

<http://www.legislation.gov.uk/ukpga/2000/23/contents>

RIPA regulates the powers of public bodies to carry out surveillance and investigation and also deals with the interception of communications.

Copyright, Designs and Patents Act 1988

<http://www.legislation.gov.uk/ukpga/1988/48/contents>

The Copyright, Designs and Patents Act (CDPA) defines and regulates copyright law in the UK. CDPA categorises the different types of works that are protected by copyright, including:

- Literary, dramatic and musical works;
- Artistic works;
- Sound recordings and films;
- Broadcasts;
- Cable programmes;
- Published editions.

Computer Misuse Act 1990

<http://www.legislation.gov.uk/ukpga/1990/18/contents>

The Computer Misuse Act was introduced partly in reaction to a specific legal case (R v Gold and Schifreen) and was intended to deter criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. The Act contains three criminal offences for computer misuse:

- Unauthorised access to computer material;
- Unauthorised access with intent to commit or facilitate commission of further offences;
- Unauthorised modification of computer material.

Human Rights Act 1998

<http://www.legislation.gov.uk/ukpga/1998/42/contents>

The Human Rights Act puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security – it provides a right to respect for an individual's "private and family life, his home and his correspondence", a right that is also embedded within the Data Protection Act.

Equality Act 2010

<http://www.legislation.gov.uk/ukpga/2010/15/contents>

The Equality Act was introduced in October 2010 to replace a number of other pieces of legislation that dealt with equality, such as the Equal Pay Act, the Disability Discrimination Act and the Race Relations Act. The Equality Act implements the four major EU Equal Treatment Directives.

Terrorism Act 2006

<http://www.legislation.gov.uk/ukpga/2006/11/contents>

The Terrorism Act creates a number of offences in relation to terrorism. Section 19 of the Act imposes a duty on organisations to disclose information to the security forces where there is a belief

or suspicion of a terrorist offence being committed. Failure to disclose relevant information can be an offence in itself.

Limitation Act 1980

<http://www.legislation.gov.uk/ukpga/1980/58>

The Limitation Act is a statute of limitations providing legal timescales within which action may be taken for breaches of the law – for example, six years is the period in which an individual has the opportunity to bring an action for breach of contract. These statutory retention periods will inform parts of the City Corporation's records management policy.

Official Secrets Act 1989

<http://www.legislation.gov.uk/ukpga/1989/6/contents>

City Corporation members of staff may at times be required to sign an Official Secrets Act provision where their work relates to security, defence or international relations. Unauthorised disclosures are likely to result in criminal prosecution. Section 8 of the Act makes it a criminal offence for a government contractor (potentially the City Corporation) to retain information beyond their official need for it and obligates them to properly protect secret information from accidental disclosure.

Malicious Communications Act 1988

<http://www.legislation.gov.uk/ukpga/1988/27/contents>

The Malicious Communications Act makes it illegal to "send or deliver letters or other articles for the purposes of causing stress or anxiety". This also applies to electronic communications such as emails and messages via social networking websites.

Digital Economy Act 2010

<http://www.legislation.gov.uk/ukpga/2010/24/contents>

The Digital Economy Act regulates the use of digital media in the UK. It deals with issues such as online copyright infringement and the obligations that internet service providers (ISPs) have to tackle online copyright infringement.

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

<http://www.legislation.gov.uk/uksi/2011/1208/contents/made>

An amendment to the Privacy and Electronic Communications Regulations in 2011 obliged websites to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies.

Police and Justice Act 2006

<http://www.legislation.gov.uk/ukpga/2006/48/contents>

Section 39 and Schedule 11 of the Police and Justice Act amend the Protection of Children Act 1978 to provide a mechanism to allow police to forfeit indecent photographs of children held by the police following a lawful seizure.

Counter-Terrorism and Security Act 2015

<http://www.legislation.gov.uk/ukpga/2015/6/contents>

Accessing websites or other material which promotes terrorism or violent extremism or which seeks to radicalise individuals to these causes will likely constitute an offence under the Counter-Terrorism and Security Act 2015.