



# Data Protection Act 2018

## 2018 CHAPTER 12

### PART 4

#### INTELLIGENCE SERVICES PROCESSING

### CHAPTER 2

#### PRINCIPLES

##### *The data protection principles*

#### **86 The first data protection principle**

- (1) The first data protection principle is that the processing of personal data must be—
  - (a) lawful, and
  - (b) fair and transparent.
- (2) The processing of personal data is lawful only if and to the extent that—
  - (a) at least one of the conditions in Schedule 9 is met, and
  - (b) in the case of sensitive processing, at least one of the conditions in Schedule 10 is also met.
- (3) The Secretary of State may by regulations amend Schedule 10—
  - (a) by adding conditions;
  - (b) by omitting conditions added by regulations under paragraph (a).
- (4) Regulations under subsection (3) are subject to the affirmative resolution procedure.
- (5) In determining whether the processing of personal data is fair and transparent, regard is to be had to the method by which it is obtained.
- (6) For the purposes of subsection (5), data is to be treated as obtained fairly and transparently if it consists of information obtained from a person who—

---

*Status: This is the original version (as it was originally enacted).*

---

- (a) is authorised by an enactment to supply it, or
  - (b) is required to supply it by an enactment or by an international obligation of the United Kingdom.
- (7) In this section, “sensitive processing” means—
- (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
  - (b) the processing of genetic data for the purpose of uniquely identifying an individual;
  - (c) the processing of biometric data for the purpose of uniquely identifying an individual;
  - (d) the processing of data concerning health;
  - (e) the processing of data concerning an individual’s sex life or sexual orientation;
  - (f) the processing of personal data as to—
    - (i) the commission or alleged commission of an offence by an individual, or
    - (ii) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

## **87 The second data protection principle**

- (1) The second data protection principle is that—
- (a) the purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and
  - (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.
- (2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).
- (3) Personal data collected by a controller for one purpose may be processed for any other purpose of the controller that collected the data or any purpose of another controller provided that—
- (a) 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.
- (4) Processing of personal data is to be regarded as compatible with the purpose for which it is collected if the processing—
- (a) consists of—
    - (i) processing for archiving purposes in the public interest,
    - (ii) processing for the purposes of scientific or historical research, or
    - (iii) processing for statistical purposes, and
  - (b) is subject to appropriate safeguards for the rights and freedoms of the data subject.

## **88 The third data protection principle**

The third data protection principle is that personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

**89 The fourth data protection principle**

The fourth data protection principle is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

**90 The fifth data protection principle**

The fifth data protection principle is that personal data must be kept for no longer than is necessary for the purpose for which it is processed.

**91 The sixth data protection principle**

- (1) The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.
- (2) The risks referred to in subsection (1) include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.