These notes refer to the Coroners and Justice Act 2009 (c.25) which received Royal Assent on 12 November 2009

CORONERS AND JUSTICE ACT 2009

EXPLANATORY NOTES

THE ACT

Commentary on Sections

Part 8 - Data Protection Act 1998

Section 173: Assessment notices

736. Section 173 inserts new sections 41A, 41B and 41C into the 1998 Act. New section 41A(1) enables the Information Commissioner to carry out an assessment to determine whether a data controller has complied or is complying with the data protection principles. The Information Commissioner is not required to seek the consent of the data controller to undertake this assessment. Under this subsection, the Information Commissioner will be able to issue an assessment notice, which will require the subject of the notice to take certain action as set out in section 41A(3).

737. New section 41A(2) provides that the data controllers that may be served with an assessment notice are government departments, public authorities designated for the purposes of section 41A by an order made by the Secretary of State and other persons of a description so designated.

738. New section 41A(3) lists the requirements that may be included in an assessment notice. These include permitting the Commissioner to enter any specified premises and observe the processing of any personal data that takes place on the premises. The recipient of an assessment notice may be required to direct the Commissioner to any documents, equipment or other material on the premises that are of a specified description and to assist the Commissioner to view any information of a specified description that is capable of being viewed using equipment on the premises. The recipient of the notice may be required to permit the Commissioner to inspect or examine any of the documents, information, equipment or material to which the Commissioner is directed or which the Commissioner is assisted to view. The recipient may also be required to comply with any request from the Commissioner for a copy of any of the documents to which the Commissioner is directed and a copy (in a form requested by the Commissioner) of any of the information which the Commissioner is assisted to view. Finally, the notice may require the recipient to make available for interview by the Commissioner persons who process personal data on behalf of the data controller (and are willing to be interviewed).

739. New section 41A(5) sets out that the assessment notice must specify either the time when, or the period within which, the requirements of the notice must be complied with.

740. New section 41A(6) sets out that assessment notices must contain particulars of the rights of appeal conferred by section 48 of the 1998 Act.

741. New section 41A(7) provides that the Commissioner may cancel an assessment notice. This is to be done by giving a written notice to the data controller on whom the assessment notice was served.

742. New sections 41A(8) and 41A(11) oblige the Secretary of State to consider, at least every five years, whether it is still appropriate for a public authority, and necessary for a description of data controller, to be designated by order and, therefore, be subject to assessment notices.

743. New section 41A(9) provides that the Secretary of State must not designate a description of data controller as liable for assessment notices without a recommendation from the Information Commissioner. It also provides that before making an order to designate a description of data controller, the Secretary of State must consult such persons as appear to the Secretary of State to represent the interests of persons of the description to be designated and such other persons as the Secretary of State considers appropriate.

744. New section 41A(10) sets out the test that must be applied by the Information Commissioner when deciding whether to make a recommendation, and the Secretary of State when deciding whether to make an order to designate a description of data controller. They must be satisfied that designation is necessary having regard to the nature and quantity of data under the control of such persons, and any damage or distress which may be caused by a contravention by such persons of the data protection principles.

745. New section 41A(12) provides two definitions. It provides a definition of "public authority", for the purpose of the order-making power in section 41A(2)(b), as any body, office-holder or other person in respect of which an order may be made under section 4 or 5 of the Freedom of Information Act 2000 or under section 4 or 5 of the Freedom of Information (Scotland) Act 2002. This adds to and expands the definition of public authority in section 1(1) of the 1998 Act, which provides that public authority means a public authority as defined by the Freedom of Information Act 2000 or a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002.

746. Section 41B(1) provides that the time or period given for compliance with an assessment notice must allow time for an appeal to be brought under section 48 of the 1998 Act. The result of this is that the need to comply with an assessment notice will be suspended if an appeal is brought.

747. New section 41B(2) establishes an exception to section 41B(1) by virtue of which, if there are special circumstances, the Commissioner can ask the data controller to comply with a requirement in an assessment notice as a matter of urgency. In this case the notice can take effect after seven days, beginning with the day on which the assessment noticed is served. The assessment notice in this case will need to include a statement that the Commissioner considers that the notice must be complied with as a matter of urgency and the Commissioner's reasons for that conclusion.

748. New section 41B(3) ensures protection for material benefiting from legal professional privilege. An assessment notice does not have effect in relation to material that meets one of the tests set out in this subsection.

749. New section 41B(5) provides a number of exclusions from the powers to give assessment notices. They do not apply to a judge, which is defined in section 41C(6) as including a justice of the peace (or, in Northen Ireland, a lay magistrate), a member of a tribunal, and a clerk or other officer entitled to exercise the jurisdiction of a court or tribunal. In this section, tribunal means any tribunal in which legal proceedings may be brought.

750. Bodies specified in section 23(3) of the Freedom of Information Act 2000 are also excluded under section 41A(5). Those bodies are:

- the Security Service,
- the Secret Intelligence Service,
- the Government Communications Headquarters,

- the special forces,
- the Tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,
- the Tribunal established under section 7 of the Interception of Communications Act 1985,
- the Tribunal established under section 5 of the Security Service Act 1989,
- the Tribunal established under section 9 of the Intelligence Services Act 1994,
- the Security Vetting Appeals Panel,
- the Security Commission,
- the National Criminal Intelligence Service,
- the Service Authority for the National Criminal Intelligence Service, and
- the Serious Organised Crime Agency.

751. Finally, the Office for Standards in Education, Children's Services and Skills, is excluded from the scope of assessment notices, but only in so far as it is a data controller in respect of information processed for the purposes of functions exercisable by Her Majesty's Chief Inspector of Education, Children's Services and Skills by virtue of section 5(1)(a) of the Care Standards Act 2000.

752. New section 41C of the 1998 Act requires the Information Commissioner to produce a code of practice in relation to the exercise of his or her new function of issuing assessment notices. Section 41C(1) requires the Commissioner to produce the code and section 41C(2) provides a non-exhaustive list of the matters that must be covered by the code. Section 41C(3) provides that the code must make provision about access to health information and social care information. Section 41C(4) deals with the content of the report produced by the Commissioner as a result of an assessment notice. Section 41C(5) and (6) provide that the Commissioner may alter or replace the code and that such a replacement or altered code must be issued by the Commissioner. Section 41B(7) provides that any code must be approved by the Secretary of State before being issued. Section 41B(8) requires the Commissioner to publish the code.

Section 174: Data-sharing code of practice

753. This section inserts new sections 52A to 52E into the 1998 Act. New section 52A places the Information Commissioner under a duty to publish and keep under review a data-sharing code of practice.

754. New section 52A(1) and (2) provide that the code will contain practical guidance and any other guidance that promotes good practice in the sharing of personal data. Good practice is defined as practice that appears to the Information Commissioner to be desirable including, but not limited to, compliance with the requirements of the 1998 Act. When deciding what constitutes good practice, the Information Commissioner must have regard to the interests of data subjects and others.

755. New section 52A(3) requires that in preparing the code the Information Commissioner must consult, as he or she considers appropriate, with trade associations, data subjects and persons who represent the interests of data subjects.

756. New section 52A(4) defines sharing of personal data as the disclosure of the data by transmission, dissemination or otherwise making it available. For example the sending of files, the granting of access to a database and the publication of information all amount to "sharing" under this definition.

757. New section 52B(1) requires that once the Information Commissioner has prepared the code it must be submitted to the Secretary of State for approval.

758. New section 52B(2) provide that approval may be withheld only if the Secretary of State is of the opinion that the code is incompatible with any community obligations (such as EC Directive 95/46/EC on the protections of individuals with regard to the processing of personal data and on the free movement of such data) or any international obligations of the UK (such as the Convention for the protection of individuals with regard to automatic processing of personal data: Convention 108 of the Council of Europe).

759. If approval is withheld, new section 52B(3) requires the Secretary of State to publish the reasons for this. If approval is granted, the Secretary of State must lay the code before Parliament.

760. New section 52B(4) to (11) makes provision relating to the issuing of the code. In particular, either House of Parliament has 40 days (excluding any period during which Parliament is not sitting for more than four days) in which to pass a resolution refusing to approve the code. If such a resolution is passed, or if the Secretary of State withholds approval, then the Information Commissioner is obliged to prepare another code of practice for approval. Where approval is granted and no resolution is passed, the Information Commissioner must issue the code. The code then comes into force 21 days later.

761. New section 52C(1) requires the Information Commissioner to keep the code under review and empowers him or her to prepare an alteration or replacement to the code. New Section 52C(2) obliges the Information Commissioner to alter or replace the code if he or she becomes aware that application of the code could give rise to a claim that the UK was in any way in breach of its European Community or other International obligations.

762. New section 52C(3) requires the Commissioner in preparing an alteration or replacement code to consult, as he or she considers appropriate, with trade associations, data subjects and such persons who represent the interests of data subjects. New section 52C(4) provides that section 52B (with the exception of subsection (6)) applies equally to a replacement code or an alteration to the code.

763. New section 52D makes provision for the code, any replacement code and any alteration, to be published by the Information Commissioner.

764. New section 52E provides that although the code cannot of itself give rise to legal proceedings, a person's breach or compliance with the code is to be taken into account by the courts, the Information Tribunal, and the Commissioner, whenever it is relevant to a question arising in legal proceedings or in connection with the exercise of the Commissioner's functions. So, for example, the Information Commissioner is entitled to consider levels of compliance with the data-sharing code of practice when evaluating whether to instigate enforcement action in relation to an instance of data-sharing. Equally a court would be entitled to have regard to levels of compliance with the code where it was attempting to resolve an issue relating to whether or not a particular person had fulfilled their legal obligations by complying with good practice.

Section 175 and Schedule 20: Further amendments of the Data Protection Act 1998

765. This section introduces Schedule 20, which makes amendments to the 1998 Act.

Data Controllers' Registration

766. *Paragraph 1* of Schedule 20 amends section 16(1) of the 1998 Act. The Information Commissioner is obliged under section 19 of the 1998 Act to maintain a register of data controller notifications. Section 17(1) of the 1998 Act prohibits the processing of personal data unless the data controller has an entry recording his or her details in the register of data controllers. Section 18(5) of the 1998 Act provides that where a data

controller notifies the Information Commissioner, the notification must be accompanied by such fee as may be prescribed by fees regulations. Under section 19(2) of the 1998 Act each register entry shall consist of the registrable particulars of the data controller and such other information as is required by the notification regulations. The term "registrable particulars" is defined in section 16(1). The amendment in paragraph 1 adds a new registrable particular to section 16(1) of the 1998 Act (new subparagraph (h)).

767. The new registrable particular is such information about the data controller as is prescribed under new section 18(5A) of the 1998 Act. Section 18(5A) is inserted by *paragraph 2* of Schedule 20 and provides that notification regulations may prescribe the information about the data controller that is required for the purpose of verifying the fee payable under section 18(5). If false information is provided in a notification then this may be an offence under section 5 of the Perjury Act 1911, Article 10 of the Perjury (Northern Ireland) Order 1979 (SI 1979/1714 (NI 19)) or section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995.

768. *Paragraph 3* of Schedule 20 amends section 19 of the 1998 Act to add a new subsection (8). It provides that the Information Commissioner will not be required to comply with section 19(6) and (7) in relation to the information that has to be supplied under new section 16(1)(h). Section 19(6) provides for the Information Commissioner to make the register of notifications available to the public for inspection and available to the public in such other ways as he or she considers appropriate. Section 19(7) requires the Information Commissioner to provide certified copies of registrable particulars in the register of notifications to members of the public.

769. *Paragraph 4* amends section 20 of the Act to enable regulations to be made requiring data controllers to notify the Information Commissioner of any changes to their registrable particulars for the purpose of ensuring that the correct annual notification fee is paid. Data controllers will not need to provide the Information Commissioner with this information year after year whenever they pay their notification fee. Instead, they will need to provide this information only upon a change of circumstance. Any failure to comply with a duty imposed by such regulations may be an offence under section 21(2) of the 1998 Act.

770. The overall effect of these amendments is to provide a way for the Information Commissioner to check that a data controller has paid the correct notification fee.

Assessment notices

771. *Paragraphs 5 and 6* of Schedule 20 make three amendments that are consequential on the creation of new sections 41A and 41B of the 1998 Act by section 173. *Paragraph 5* amends section 48 of the 1998 Act to provide a right of appeal to the tribunal against an assessment notice. Paragraph 6 amends section 67 of the 1998 Act to specify the parliamentary procedure that is to be followed by the Secretary of State in making orders under the power in new section 41A(2)(b) (power to designate specific public authorities as being within the scope of Assessment Notices) and 41A(2)(c) (power to designate a person of a description as being within the scope of Assessment Notices). Such orders will be subject to the negative resolution procedure and the affirmative resolution procedure respectively. *Paragraph 7* inserts a new definition of government department into section 70(1) of the 1998 Act.

Power to require information

772. *Paragraph 8* of Schedule 20 amends section 43 of the 1998 Act to strengthen the Information Commissioner's powers for inspecting a data controller's compliance with the data protection principles, using an information notice.

773. *Paragraph 8*(3) inserts two new subsections into section 43 of the 1998 Act, which contains the power of the Information Commissioner to issue an information notice. New section 43(1A) allows an information notice to require that the data

controller must provide (a) particular information as specified; (b) information of a particular description; or (c) information in a category as specified or described. New section 43(1B) allows an information notice to require that the information is provided (a) within a specified period; (b) at a specified time and place; (c) in a specified form.

774. *Paragraph 9* provides an equivalent amendment (to that made in paragraph 8 detailed above) to section 44 of the 1998 Act for special information notices (which makes special provisions in relation to the processing of personal data for journalistic, artistic and literary purposes).

Restriction on the use of information

775. *Paragraph 10* of Schedule 20 amends section 43 of the 1998 Act to place restrictions on the use of certain information obtained under the newly extended information notice power.

776. Paragraph 10(3) inserts three new subsections into section 43 of the 1998 Act. These subsections make provision to ensure that the principle against self-incrimination is protected in relation to this section. First, the new section prohibits a data controller from being required to provide information which would incriminate him or her in relation to proceedings other than proceedings for offences under the 1998 Act, and certain perjury offences. Second, statements made under the new expanded power of section 43 cannot be used as evidence against the data controller for any data protection offence (other than the offence of failing to comply with the terms of an information notice), unless the accused acts in such a way as to forfeit this particular protection. In those circumstances evidence of the original statement would be admissible in order to rebut the false assertions made by the accused.

777. *Paragraph 11* of Schedule 20 provides for an equivalent amendment to that made in paragraph 10 to be made to section 44 of the 1998 Act relating to special information notices (which makes special provisions in relation to the processing of personal data for journalistic, artistic and literary purposes).

778. *Paragraph 12* of Schedule 20 amends paragraph 11 of Schedule 7 to the 1998 Act to make provision in relation to the principle against self-incrimination. This existing provision of the 1998 Act provides that data controllers are not obliged to satisfy subject access requests under section 7 of the 1998 Act, where to do so would reveal incriminating evidence of an offence other than an offence under the 1998 Act. The amendment adjusts the provisions so that neither the 1998 Act offences nor certain perjury offences are covered by this protection.

Monetary penalties: restriction on matters to be taken into account

779. Section 55A of the 1998 Act provides for the Information Commissioner to issue a monetary penalty for serious breaches of the data protection principles of a kind likely to cause substantial damage or distress that are carried out either deliberately or recklessly.

780. Under section 51(7) of the 1998 Act the Information Commissioner can, with the consent of the data controller, assess any processing of personal data for the following of good practice.

781. *Paragraph 13* of Schedule 20 amends section 55A of the 1998 Act to prevent the imposition of a monetary penalty based on information that has been obtained from a good practice assessment (section 51 of the 1998 Act) or the use of an assessment notice under new section 41A of the 1998 Act as inserted by section 173.

Warrant for entry and inspection

782. *Paragraph 14* of Schedule 20 amends Schedule 9 to the 1998 Act to give broader inspection powers to the Information Commissioner in relation to warrants obtained under Schedule 9 to the 1998 Act.

783. Paragraph 14(2) amends paragraph 1 of Schedule 9 to give a circuit judge or a District Judge (Magistrates' Courts) the power to grant a warrant to the Information

Commissioner on the grounds that a data controller has failed to comply with the requirements of an assessment notice.

784. Paragraph 14(3) broadens the range of activities the Information Commissioner can engage in when executing a warrant granted under Schedule 9. In particular, it gives the Information Commissioner the power to require any person on the premises to provide an explanation of any document or other material found on the premises (new paragraph 1(3)(e)) and to require such a person to provide information that is reasonably required to determine whether there has been any contravention of the data protection principles (new paragraph 1(3)(f)).

785. Paragraph 14(4) and 14(5) provide for amendments to Schedule 9 to the 1998 Act that are consequential on the introduction of warrants for failure to comply with an assessment notice. Under the amendments in paragraph 14(4) the requirement in paragraph 2(1)(a) of Schedule 9 to the Data Protection Act 1998, that before a warrant can be issued the Information Commissioner must give seven days' notice in writing to the data controller demanding access to the premises, cannot be satisfied by serving a data controller with an assessment notice. The amendment in paragraph 14(5) reflects the fact that the new test for granting a warrant would not be dependent on the Information Commissioner finding evidence on the premises to be searched.

786. Paragraph 14(6) makes amendments to paragraph 12 of Schedule 9 to the 1998 Act, which provides a criminal offence for the obstruction of, or failure to assist, a person executing a warrant under that Schedule. The additional text extends the offence to cover deliberately or recklessly making false statements in response to the new powers to require information created in paragraph 14(3) detailed above.

787. Paragraph 14(7) provides protection against self-incrimination for any person required to provide information under the extended powers created under paragraph 14(3) above. In particular, any information provided by that person in response to these new powers under a warrant cannot be used as evidence in criminal proceedings against that person. However, this protection is not absolute, and the response given can be used in evidence if the offence concerned is either the offence of obstructing or failing to assist a person executing a Schedule 9 warrant or is one of a specific group of perjury offences. Furthermore the response can be used in evidence for the prosecution of any criminal offence if the accused acts in such a way as to forfeit this particular protection. In those circumstances evidence of the original statement becomes admissible in order to rebut the false assertions made by the accused.