Justice Committee

Criminal Cases (Punishment and Review) (Scotland) Bill

Letter from the Cabinet Secretary for Justice to the Convener

Thank you for your letter of 20 December in relation to the Criminal Cases (Punishment and Review) (Scotland) Bill (“the Bill”).

For ease of reference, the Committee’s comments are copied below followed by our response to each of the points raised.

Justice Committee comments
First, the Committee would welcome clarification on what you and your advisers understand those data protection obstacles to be. We make this request in the awareness that data protection law is complicated, and that some further pointers as the precise legal factors potentially preventing disclosure of information would help us understand the underlying issues and interrogate the evidence more effectively.

Scottish Government response
As you’ll be aware, the Scottish Government has not seen the contents of the Statement of Reasons (“SoR”) produced by the Scottish Criminal Cases Review Commission (“the Commission”) in the Al-Megrahi case. However, based on discussions with the Commission, our understanding is that the data protection obstacles that currently exist, and that would not be affected by the Bill (and therefore will continue to exist even if the Bill is passed), relate to what is known as, under data protection legislation, ‘personal data’ and ‘sensitive personal data’.

As you note, data protection legislation is complex, but hopefully the following information is helpful in understanding the relevant issues. Under section 1(1) of the Data Protection Act 1998 (“the DPA”), personal data is defined as data which relate to a living individual who can be identified –

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

The definition of personal data 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 by section 2 of the DPA as personal data consisting of information as to –

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
• his sexual life,
• the commission or alleged commission by him of any offence, or
• 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.

Processing, in relation to information or data, is defined in section 1 of the DPA as
obtaining, recording or holding the information or data or carrying out any operation
or set of operations on the information or data, including –

• organisation, adaptation or alteration of the information or data,
• retrieval, consultation or use of the information or data,
• disclosure of the information or data by transmission, dissemination or
  otherwise making available, or
• alignment, combination, blocking, erasure or destruction of the information or
  data.

In the context of the Commission and the Bill, processing would refer to the potential
disclosure of the information.

The conditions for processing of information are set out in Schedules 2 and 3 to the
DPA. Unless a relevant exemption applies, at least one of the following conditions
must be met whenever personal data is processed:

• The individual who the personal data is about has consented to the
  processing.
• The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can
    enter into a contract.
• The processing is necessary because of a legal obligation that applies to you
  (except an obligation imposed by a contract).
• The processing is necessary to protect the individual’s “vital interests”. This
  condition only applies in cases of life or death, such as where an individual’s
  medical history is disclosed to a hospital’s A&E department treating them after
  a serious road accident.
• The processing is necessary for administering justice, or for exercising
  statutory, governmental, or other public functions.
• The processing is necessary for the purposes of legitimate interests pursued
  by the data controller or by the third party or parties to whom the data are
  disclosed, except where the processing is unwarranted in any particular case
  by reason of prejudice to the rights and freedoms or legitimate interests of the
  data subject.

In addition, if the information is sensitive personal data, at least one of several other
conditions must also be met before the processing can comply with data protection
legislation. These other conditions are as follows:
The individual who the sensitive personal data is about has given explicit consent to the processing.

The processing is necessary so that you can comply with employment law.

The processing is necessary to protect the vital interests of:
- the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
- another person (in a case where the individual's consent has been unreasonably withheld).

The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.

The individual has deliberately made the information public.

The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.

The processing is necessary for administering justice, or for exercising statutory or governmental functions.

The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.

The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

We understand from the Commission that there are a significant number of items of both personal data and sensitive personal data contained throughout the SoR in the Al-Megrahi case. Before disclosing personal data, the Commission would require to ensure that they have met at least one of the conditions contained in the relevant list above. Before disclosing sensitive personal data, the Commission would require to ensure that they have met at least one of the conditions contained in each of the two lists of conditions above.

When processing personal data, it should be noted that in order to comply with the sixth condition in Schedule 2 (the "legitimate interest" condition) the data controller is required to balance that legitimate interest with the rights and freedoms, or legitimate interests, of the data subject(s) in question.

It should also be noted that compliance with a condition of Schedule 2, or as the case may be, Schedule 3, does not absolve the data controller of their obligation to comply with the first principle, that data should be processed fairly and lawfully. In other words, it is still possible to contravene the first principle even where the processing has an otherwise lawful basis under Schedules 2 and 3.

We understand from the Commission that they consider that obtaining consent (i.e. the first condition on both lists) is the only realistic means of meeting the requirements of data protection legislation to allow disclosure of information which consists of personal data or sensitive personal data. This runs counter to the intention of the Bill which is intended to provide discretion to the Commission to decide whether it is appropriate in the whole circumstances of a case to disclose information. With the exception of information obtained under international obligations, the Bill does not require the Commission to obtain content from either those who provided information or who are mentioned.
In summary, without steps being taken to remove data protection obstacles as outlined above, our understanding is that it will be very difficult for the Commission to be able to disclose information in the Al-Megrahi case, even if the Commission decided it was appropriate to do so under the terms of the Bill, without being in breach of the DPA.

Part V of the DPA deals with enforcement. There is no stand-alone offence within the Act for a failure to comply with the data protection principles, however, section 55A provides the Information Commissioner with the power to serve a civil monetary penalty notice on a data controller who is in contravention of the data protection principles, where that contravention is of a kind likely to cause serious damage or distress to the data subject. The maximum monetary penalty is £500,000.\(^1\)

**Justice Committee comments**

Secondly, the Committee appreciates that much of data protection law derives in turn from European law, which sets out key principles of data protection that must generally be adhered to within all member states. Again, we would welcome clarification on what you and your advisors understand to be the areas where the UK Government would have a discretion to permit derogation from the rules ordinarily restricting the disclosure of the relevant information.

**Scottish Government response**

The Data Protection Directive (95/46/EC) (“the Directive”)

This Directive is the principal instrument regulating data protection within the European Union. The DPA was passed by the U.K. Government in order to fulfil its obligations under the Directive. For that reason, the DPA follows the Directive fairly closely. For example, the conditions contained in Schedules 2 and 3 of the DPA transpose the conditions contained in Articles 7 and 8 of the Directive. The Directive therefore also recognises that there are occasions where the processing of personal data and sensitive personal data has a legitimate basis.

The question of the extent of harmonisation of the Directive (that is, the extent to which member states have the ability to implement its obligations in different ways) has been considered in the case of *Lindqvist*. In that case, the question was whether the Directive was designed to achieve “maximum” harmonisation within member states. If so, this would require member states to implement the Directive exactly, by providing national protection that was neither stronger nor weaker than that in the Directive.

The European Court of Justice’s response was that it was open to member states to meet the requirements of the Directive but also to exceed them, suggesting that maximum harmonisation was not required. The court did not address a derogation from the Directive. Whether or not such derogations are possible is a matter for the UK Government to consider.

\(^1\) Data Protection (Monetary Penalties (Maximum Penalty and Notices) Regulations 2010 (SI 2010/31), reg 2

\(^2\) *Lindqvist* (C-101/01) [2003] ECR I-1297 at para [99]
Order making power - DPA

Under paragraph 10 of Schedule 3 of the DPA, the UK Government has an order-making power to specify further circumstances in which sensitive personal data can be processed.

The use of such an order-making power could potentially allow sensitive personal information to be disclosed without the consent of the data subject and without falling foul of data protection legislation. In asking the UK Government to consider whether they think it would be appropriate to disapply data protection legislation in this way, we are aware of a number of complex issues to be considered, including adhering to the requirements of the Data Protection Directive. These are matters for the U.K. Government to consider, however it is likely that any circumstances specified by such an order would require there to be evidence that the processing of the sensitive personal data is in “the substantial public interest”.

Justice Committee comments

Thirdly, the Committee is not certain as to whether there are other legal rules than data protection law that might restrict the Commission’s ability to publicly disclose particular information relating to the Megrahi case. For instance, we are unclear whether the Official Secrets Acts might apply or whether there are any common law protections that might potentially be available to interested parties. It would be helpful to the Committee if you were able to set out your thoughts on this issue.

Scottish Government response

We would draw your attention to paragraph 24 of the explanatory notes for the Bill. This states:

‘Whether information is actually released turns principally on the appropriateness test under section 194M(1)(b). As well as the matters referred to in section 194M(3) though, it should be noted that the Commission’s ability to disclose information will be informed (and may be restricted) by the application of ECHR law and the operation of reserved statutes such as the Data Protection Act 1998 and the Official Secrets Acts 1911-1989.’

As noted previously, the Scottish Government has not seen the SoR produced by the Commission in the Al-Megrahi case. It is therefore difficult to say with any degree of absolute certainty that, for example, official secrets legislation will be relevant, but it is thought likely such legislation will, at the very least, need to be considered depending on the nature of the information in the SoR.

Under Article 8 of the ECHR, which is relevant to Scots law by virtue of section 1(2) of the Human Rights Act and section 57(2) of the Scotland Act 1998, everyone has a

---

3 This wording is used in the principal previous order made under this paragraph, the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417). Four further orders have been made under this paragraph to date – SI 2002/2905, SI 2006/2068, SI 2009/1811 and SI 2010/2961.
right to respect for his private life and family life, his home and correspondence. Under section 6 of the Human Rights Act, it is unlawful for a public authority to act in a way that is incompatible with a Convention right.

In respect of any common law protections, breach of confidence and privacy rights may well be relevant considerations (though again this depends on the nature of the information in the SoR). It should be noted that common law actions for breach of confidence and privacy tend to arise in cases between private persons, because Article 8 has no direct horizontal effect (a human rights claim cannot be raised directly against a private body – in such a case there must be a prior cause which enables the claim to reach court).

There is unlikely to be a need for an affected person or interested party to raise a common law action for breach of privacy against the Commission, which is a public authority within the meaning of section 6 of the Human Rights Act, because they could raise a human rights claim directly.

I hope this information is helpful to the Committee.

Kenny MacAskill MSP
Cabinet Secretary for Justice
23 January 2012