BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 8, Number 8 August 2008

Data protection and health related data: recent European developments and possible wider implications for barnardised data

By Pierre-Andre Dubois (Partner) and Shannon Yavorsky (Associate), Kirkland & Ellis International LLP. The authors can be contacted at: pdubois@kirkland.com and syavorsky@kirkland.com

Two recent cases, one heard by the U.K. House of Lords (*Common Services Agency v. Scottish Information Commissioner)* and the other by the European Court of Human Rights ("ECHR") (*I v. Finland)* (see also News 'Finland' in this issue) have considered issues around privacy and medical data. Although the decisions come at the issue of personal health data from different angles, both decisions highlight the importance of heightened vigilance by public bodies when processing or considering processing health data. Interestingly, these cases involve public bodies at different ends of the compliance spectrum: whilst the *I v. Finland* case concerns the failure by a public body to provide adequate protection for personal data, the *Common Services Agency* case is an example of a public body exercising an abundance of caution with respect to protecting personal data when faced with a request for access under freedom of information legislation. It may be that reading these cases in tandem will provide some guidance on where the balance is to be struck between adequately protecting data and appropriately disclosing it. Furthermore, the *Common Services Agency* case has left the question open as to whether barnardised data is actually anonymous data excluded from data protection laws.

Common Services Agency v. Scottish Information Commissioner

In a case involving data relating to incidents of childhood leukaemia, the House of Lords confirmed that public authorities can be required to anonymise personal data and that, in so doing, they are not to be viewed as creating new information. However, in rendering its decision, the House of Lords declined to confirm whether certain information constitutes personal data and whether such information should be processed. The Lords talked around the issues and sent a host of questions back to the Scottish Informa-

tion Commissioner who must now determine these issues in view of the guidance provided by the Lords.

Background

The Common Services Agency (the "CSA") is a Scottish public body which is tasked with collating and disseminating epidemiological information. In January 2005, a request was made by Mr Collie (acting on behalf of Chris Ballance who was then a member of the Scottish Parliament) to the CSA to provide details of all incidents of childhood leukaemia from 1990 to 2003 for two postal areas. It was not disputed that there was a general public interest in such information since there was a nearby decommissioned nuclear reactor and nuclear processing facilities which had been the subject of health concerns for many years. The CSA refused this request on the basis that the information from 2002 to 2003 was incomplete and, with respect to the earlier years, it took the view that there was a significant risk of identifying living individuals as a result of the low number of subjects, the specified age group and the small geographic area. As a result, it concluded that the information was personal data within the meaning of the U.K. Data Protection Act 1998 (the "Act") and was exempt information for the purposes of the Freedom of Information (Scotland) Act 2002. The CSA also claimed that it owed a duty of confidence equivalent to that of the clinicians to whom the information had originally been made available.

The decision of the Scottish Information Commissioner

Mr Collie appealed to the Scottish Information Commissioner. The Commissioner was satisfied that the requested information constituted personal data under the Act. Further, he noted that the disclosure of the information would breach the first data protection principle since it would be both unlawful (as a result of the breach of confidence) and unfair (since a person would not expect their diagnosis of leukaemia to be placed in the public domain). However, the fact that the disclosure of the information would be unlawful and unfair did not in itself mean that the information should not be disclosed to Mr Collie. He said that the information could be "barnardised" *i.e.* presented in manipulated form so as to reduce the likelihood of identification of individuals. The Commissioner therefore ordered the CSA to provide Mr Collie with the information in barnardised form.

Court of Session

The CSA appealed to the Court of Session. The First Division of the Court of Session refused the appeal. It held that a table setting out the data, barnardised in the form described by the Commissioner, would not constitute personal data for the purposes of the Act. It was information held by the CSA at the time when the request was received and the Commissioner was entitled to order the CSA to disclose it.

House of Lords

There were several issues raised by the appeal against the decision to the House of Lords. The first issue for the court was whether the information which the Commissioner ordered the CSA to release in barnardised form to Mr Collie was "held" by the CSA? If so, would information in this form constitute "personal data" and if it was, would the information also constitute sensitive personal data? Finally, if it was sensitive personal data, would its release to Mr Collie meet one of the conditions for processing sensitive personal data?

Was information ''held'' by the CSA?

The CSA argued that the process of barnardisation would require the production or making of information that was different from that which was held by it at the time of the request. It submitted that the process required information to be created and until this was done, it was not "held" by the CSA. The House of Lords disagreed holding that information in barnardised form would contain information that was "held" by the CSA at the time of the request, and unless it was "personal data" and its disclosure would contravene any of the data protection principles, it would have to be released in response to it.

Does the information in barnardised form constitute personal data?

The House of Lords did not answer the question as to whether or not the barnardised data was personal data. It remitted this question to the Commissioner for him to determine as a question of fact. The House of Lords, however, unanimously confirmed that data which is anonymous is not subject to data protection (as stated in Recital 26 of the Data Protection Directive). What the decision did not define was what would be needed to done through barnardisation to ensure that the data became truly anonymous. Although the Commissioner had ordered the CSA to release the barnardised data, his decision had not considered whether such data was personal or whether it could be released under the Act.

Does the information in barnardised form constitute ''sensitive'' personal data?

The House of Lords also refrained from answering the question of whether the barnardised data could constitute sensitive personal data. This question was referred back to the Commissioner for him to determine as a question of fact. However, the House of Lords noted that it would seem a short step to conclude that if the barnardised data was personal data then it must be sensitive personal data too since it was data about the physical health of living children who could be identified from data released in response to the request together with other information held by the CSA.

   ISSN 1473-3579

Would the release of such personal data to Mr Collie meet one of the conditions for processing personal data?

The House of Lords indicated that when determining the issue of releasing the data, the Commissioner should consider whether the release would: (i) be fair and lawful; (ii) meet one of the conditions set out in Schedule 2 of the Act; and (iii) if the information was sensitive personal data, meet one of the conditions set out in Schedule 3 of the Act.

The Scottish Information Commissioner

The Scottish Information Commissioner has been given a lot to chew on and it will be interesting to see how he answers these questions in light of the guidance provided by the House of Lords. Although the House of Lords may have asked more questions than it answered in this case, it did confirm that public authorities can be required to anonymise data and that in doing so they are not creating new information. This decision will at least assist public authorities in determining whether they "hold" information.

Case of I v. Finland

The applicant in this case, a Finnish women referred to as "I" to protect her anonymity, worked as a nurse from 1989 to 1994. She was HIV-positive and regularly attended a clinic within the same hospital in which she was employed. In 1992, she began to suspect that her colleagues were aware of her condition. At the time, hospital staff had free access to the patient register which contained information on patients' health status. In 1992, the records were made available only to the treating clinic's personnel. I's name was changed on the register.

In 1996, I asked the Country Administrative Board to tell her who had accessed her confidential patient record. The hospital was unable to provide this information since it only kept details of the last five people to access a record. I brought civil proceedings against the District Health Authority claiming damages for the alleged failure to keep her patient record confidential. The District Court and the Court of Appeal rejected the action since they were unable to find evidence that her patient record had been unlawfully consulted. I applied to the ECHR alleging a violation of Article 8 of the European Convention on Human Rights (the "Convention"), which guarantees an individual's right to respect of his private and family life.

Protection of personal data is a guaranteed right

The ECHR held that there had been a violation of I's rights under Article 8(1) of the Convention and awarded damages. The ECHR held that although the object of Article 8 was essentially to protect the individual against arbitrary interference by the public authorities, it could involve an obligation to adopt measures designed to secure respect for private life even as between individuals. I complained that there was a failure on the part of the hospital to guarantee the security of her data against unauthorised access, or in Convention terms, a breach of the State's positive obligation to secure respect for her private life by means of a system of data protection.

The ECHR confirmed that the protection of personal data, and in particular medical data, was of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8. The ECHR held that this was a particular concern in this case since the health data in question was HIV infection and sensitive issues existed around this disease.

The ECHR noted that at the relevant time, there were privacy laws in Finland that required the protection of medical data. Personal data had to be secured against, among other things, unlawful access. The data controller was also tasked with ensuring that only the personnel treating a patient had access to his or her medical record.

The need for adequate security measures

The ECHR pointed out that I had lost her civil action because she was unable to prove on the facts a causal connection between the deficiencies in the access security rules and the dissemination of information about her medical condition. However, the ECHR pointed out that to place such a burden of proof on the applicant was to overlook the deficiencies in the hospital's record keeping at the material time. It was clear that if the hospital had provided a better system for data protection, I would have been in a better position before the domestic courts. Interestingly, the ECHR noted that the mere fact that domestic data protection legislation provided I with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data, this was not sufficient to protect her private life. What was required was practical and effective protection to exclude the possibility of unauthorised access in the first place. The ECHR held that since I's medical data were not adequately secured against unauthorised access at the material time, the State failed in its positive obligation under Article 8 to ensure respect for I's private life.

Conclusion

Both of these cases highlight the fact that medical data must be adequately protected. In *I v. Finland*, the ECHR establishes a clear duty of public bodies to implement measures to keep data confidential. Arguably the most important lesson in this case is that the existence of data protection legislation (and remedies available under such legislation) is not sufficient to ensure compliance with the State's obligation under Article 8 unless measures are taken to protect personal data from unauthorised access and disclosure. This decision may place more pressure on the State to ensure that such measures are in place to protect personal data since if they fail to do so, they could incur liability under the Convention. Private businesses dealing with sensitive personal data

should also take note of the ECHR's decision as no doubt it will be used as a precedent when looking at how one should protect sensitive personal data. In *Common Services Agency v. Scottish Information Commissioner,* the issue was rather one of whether the CSA was exercising too much caution in not disclosing data in response to a request for access under freedom of information, but the decision has arguably created uncertainty around barnardised data. The decision clearly suggests that in order for data to be treated as anonymous, barnardisation will need to be extensive before one can feel comfortable that it is not caught by personal data protection. Again, while this decision involved a public authority, private businesses who, for example, collect and offer for resale or analysis data for market studies should examine the processes they use to render such data anonymous.

   ISSN 1473-3579