

MacRoberts

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LH
By email to contact(WdatasharinQreview.QsLQov.uk

Dear Sirs

Data Sharing Review

We are pleased to have this opportunity to respond to your consultation paper on the use and sharing of personal information in the public and private sector.

MacRoberts is a commercial law firm based in Scotland, with offices in Glasgow and Edinburgh. Our technology media and communications unit, which is headed by *****, has considerable experience in advising an array of clients in the public and private sector and both Mr ***** and senior associate, *****, regularly provide advice on data protection and freedom of information matters.

Scope of personal information sharing. including benefits. barriers and risks of data sharing and data protection

We believe the sharing of personal information in the public sector is essential for the effective administration of the state and the provision of public services such as health care, social services, collection and assessment of taxation and law enforcement. Additionally, in both the public and private sector there is a significant convenience dividend for consumers and organisations alike when there is a smooth transfer of data between all of the parties engaged in the provision of services.

There are many benefits to be had by public and private organisations sharing personal information. For example, in health care, it is essential that a patient's data is shared expediently with the relevant health care professionals. This benefits patients in a number of ways ranging from saving time in the consultation room to saving lives in the accident and emergency ward. The eHealth project proposed by the European Union, where patients' health information can be shared with health care professionals in other Member States, presents not only great opportunities for data sharing but also many benefits to patients throughout the European Union. Alongside those studying abroad or travelling on business or holiday, there is much economic migration in our society today and so it can only help to improve the level of care these groups receive outside of their own state when their medical history can migrate with them.

The eHealth project is an example of the future of data sharing. However, society has benefited for many years from data sharing and it is important that the implications for traditional data sharing methods are considered in any proposals that may come out of this consultation. The disclosure of a job applicant's criminal history to a potential employer, is an example of established and effective data sharing between the public

and private sector (through Disclosure Scotland and the Criminal Records Bureau in England and Wales) which offers protection to society and in particular to the most vulnerable persons within our society.

There is, however, a line in the sand (albeit a sometimes moving one) beyond which the benefits to the individual and society do not justify the sharing of personal data and instead represent an unwarranted intrusion into personal privacy.

Logically there is an inherent risk to the security of data when it is shared across national networks and international borders. Any time data is made available to another organisation or transferred electronically or physically there is the risk that security may be breached and the data may be lost, damaged, destroyed, stolen, unlawfully processed or received by an unintended recipient. There are a number of risks associated with organisations linking their databases together. These databases will present a natural target for hackers and fraudsters and could facilitate data profiling by the combination of personal information from different sources.

An increase in the volume of personal information being shared across vast networks and even greater distances, together with the linking of databases and the sharing of new types of information (such as biometric data or data relating to an individual's location from RFID technology), will further increase the risk to personal privacy and even personal safety.

The Home Office has identified that the United Kingdom's DNA database is the largest of any country in the world, containing 5.2% of the population's DNA. The retention of DNA samples taken from everyone in police custody regardless of whether any charge or proceedings follow is excessive and is one example where a public authority holds too much personal data. We note from the Home Office website that there are no plans to introduce a voluntary or compulsory DNA database for all citizens. However, we are concerned by the Government's proposals to share the DNA database with law enforcement agencies in Europe and the USA.

It is our opinion that a number of employers in the private sector hold too much personal information on their employees. Quite apart from the debate over whether an employee can ever provide free and explicit consent in the context of employment, employees and candidates for employment are often required to submit intimate personal information which is of little or no relevance to their employment. We feel this is one area where private organisations hold too much personal information.

Furthermore, we are concerned by the increase in the use of biometric data as a means of security and identification or identity verification. In particular, the use of this technology in schools which may be disproportionate and will ultimately serve to desensitise youngsters to the dangers of surveillance and the issues surrounding data protection and personal privacy. For example, whilst such measures will verify identity, it will not prevent the individual from attending school with a weapon and using it. Such measures only verify, they do not protect.

The legal framework

In our opinion the principles of the Data Protection Act (DPA) represent the principles by which personal data should be processed. Whilst the DPA is a complex piece of

legislation and is often viewed as cumbersome and by its very nature acts as a prohibition against disclosure/sharing, it is the lack of awareness of, compliance with and ineffective enforcement of the principles that act as a barrier to the effectiveness of the DPA.

The DPA lacks teeth and accordingly there is a lack of compliance from the private and public sectors. The Information Commissioner is poorly funded and has insufficient resources and powers at his disposal to enforce the DPA. It is suggested that greater enforcement and increased sanctions would be one way of increasing compliance.

That being said we have to be wary of such financial sanctions and who is targeted. Whilst there is clearly benefit to be had from better data protection throughout government, there seems little benefit to the general public in removing funds by way of fines from the budgets of such bodies. Perhaps fines should be imposed personally on responsible civil servants and/or ministers.

However, it appears inevitable that advances in technology will consign the DPA to no more than a statement of good practice, if that is not indeed already the current position.

It is our experience that many public and private organisations do not always adhere to the second principle of the DPA as well as they might. The second principle is particularly valuable as it holds organisations to processing the data for the purposes they set out in their fair processing notice. Without this principle organisations would be able to process data for unspecified and unlimited purposes. In relation to data sharing, fair processing notices should make clear that personal data may be shared with other organisations, when the data will be shared and for what purposes and any other relevant information about the data sharing. A sufficient fair processing notice and increased data subject rights may be more appropriate than imposing an additional requirement to seek the individual's consent.

The Information Commissioner's Framework code of practice for sharing personal information and the Privacy Impact Assessments (PIA) make clear what the ICO considers to be good practice. However, data controllers are under no obligation to comply and therefore, we believe that data sharing is not subject to sufficient transparency, scrutiny and accountability. This may be remedied if data controllers intending to share personal data were required to notify the Information Commissioner with details of their data sharing proposals, including to whom the data will be shared, the security measures and procedures they have put in place and the results of their own PIA.

The Information Commissioner could then approve schemes or notify the data controllers of changes he would like to see implemented to increase data security. Data controllers could then be allowed a set period of time to implement these changes whilst sharing data so as not to impact on the benefits to the organisation and the data subjects.

In the Netherlands, the data controller, when registering with the national data protection authority, has to provide a general description of the processing to allow a preliminary assessment of the suitability of the measures planned to guarantee the security of the processing. A similar system would be of benefit in the UK.

Consent and transparency

From our own experience of assisting clients on whether and when they require individuals' consent to share personal information, and what form that consent should take, it appears the issue is not clear to data controllers.

Technology

It may be beneficial to mandate specific technical safeguards by law to protect the personal information. However, a blanket requirement, for example, that all personal information held on portable devices or transferred electronically between organisations should be encrypted to a specific standard may be unfeasible and represent a significant burden for data controllers. Certain personal data will be a matter of public record and unlikely to be the source of any great harm if unlawfully processed; therefore, it would be unfair to require data controllers to encrypt this type of data. It may be more appropriate for the Information Commissioner to issue specific guidance as to the type of technical safeguards that should be implemented in certain situations, for example, Personal information containing financial or health information should be encrypted and access limited by password protection.

International Comparisons

In addition to the measures in the Netherlands discussed above, in Germany the German Federal Data Protection Act (Bundesdatenschutzgesetz) (the "BDSG") lists the technical measures in an Annex to its Article 9. They include measures on access control, transmission control, input control, processor control, availability control and separate processing. In addition the data controller is also required by the BDSG to take reasonable steps to ensure the reliability of any of his employees who process the personal data. The BDSG imposes a statutory confidentiality obligation on persons employed in data processing which survives the termination of the employment. In so far as they work for private bodies, on taking up their duties, such persons also have to give a written undertaking to maintain such confidentiality.

Perhaps these are measures the UK could take into consideration although not in respect of all data controllers but perhaps on those with more than a specified number of employees

Thank you for allowing us this opportunity to participate in the consultation exercise.