

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

Comments: a) The CPS collects holds and shares criminal case details, covering all aspects of the sensitive personal data criteria as outlined in the DPA 1998. The information is collected and shared with Police, Bar, defendants, Defence Solicitors, and other criminal justice agencies, such as the Courts Service, Probation Service and Prison Service, and is held in electronic records and on paper. We hold the information to review and prosecute offenders, and to aid the administration of justice, in accordance with the Prosecution of Offenders Act 1985.

b) The CPS holds staff details, ranging from names, addresses and date of birth, to pension details, trade union membership and medical records, covering all aspects of the sensitive personal data criteria as outlined in the DPA 1998. Personal information is collected and shared by staff, and the information is held in electronic records and paper records. The information is held for the purposes of managing staff, including ensuring payment, pension and welfare are appropriately catered for.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2.

Comments: Individual

Ensuring that victims of crime see their offenders brought to justice
Reassurance that victims and witnesses are treated appropriately and do not have to experience further distress as a result of the prosecution process
(Witness Care Units)

Society

Providing confidence in the progression of justice through the criminal justice arena

Question 3.

Comments: Individual

Fear of data being misplaced/misused
Vigilantism

Society

Distrust in the criminal justice system
Lack of confidence in the Government
Vigilantism

Question 4.

Comments: We consider that the sharing of personal information allows for the opportunity to tie up cases across the country with e-records, such as case management systems. Although we also consider that the viewing of data that is not necessary for an individual's role is a risk and could lead to misplacement of data, selling of personal data, and at the extreme corruption of staff.

Question 5.

Comments: We consider that most public authorities hold enough data, and not too much, as they will be governed by retention policies and costs available for storage. These policies will ensure that only personal information that needs to be retained for business/operational purposes will be retained for as long as is necessary and then destroyed.

Question 6.

Comments: We consider that private organisations such as supermarkets hold too much information on their store cards. They are unregulated with regard to the information they do hold about an individual, and there is no regulation to govern what personal information they do process, and for what purpose.

Question 7.

Comments: We consider that the sharing of information in relation to two public bodies, where this is not already taking place is not clear. Due to the functions of some businesses, the legality of who they share information with, and when needs to be made clearer. We consider that barriers such as legal, financial and institutional are mainly to blame. We believe that this is mainly a problem where the individual's consent is not needed and where information should be shared to safeguard an individual.

Question 8.

Comments: We consider that catalogue companies/financial institutions share information all the time, and without the individual's consent. These particular organisations allow for an individual to opt-out only, which we believe should be changed. Often, the opt-out criteria are so small and easily missed, and the opportunity to withdraw consent not fulfilled. We believe that this should be changed to opt-in for information sharing, so that the individual is aware of that his/her personal information may be shared wider.

Section 3: The legal framework

Question 9.

Comments: We consider that the Act works relatively well on balance:

Strengths

Protection of personal data – ensures privacy

Clear access regime for those requesting personal information held by an organisation

Fee

Consent provisions

Weaknesses

Act is very unfriendly to use with difficult terminology

Definition of personal data is unclear, and has been clouded further by ICO's recent guidance.

Disclosure provisions v non-disclosure provisions in the Act are very unclear. It would be helpful to have this information set out in a similar way to FoIA.

The disclosure provisions do not take into account other disclosure regimes, eg, Criminal Proceedings and Investigations Act

Disproportionate effort needs more guidance

Structured filing system needs more guidance

Question 10.

Comments: We believe that the intention of the second principle is very valuable, but would be better enhanced if enforcement was more rigorous. There is a conflict with regard to data sharing in some parts of the public sector, but mainly in the private sector. Again we believe this to be due to the lack enforcement, but also lack of regulation in the private sector. Additionally, we believe that the registration (notification process) is over complicated and requests too much from those registering; we consider that the process needs to be simplified.

Question 11.

Comments: We consider that the Act has not kept pace with technological advances in society – it focuses too much on paper records. For example, the DPA is based only on material held in the UK and is landlocked. There is no provision for database that are based outside the UK. We consider that this conflicts with freedom of expression that is paramount to the majority of international society.

Question 12.

Comments: We believe that sanctions should be settled in civil courts and the Commissioner should take a more active role in the delivering of penalties when compliance has been breached.
More accountability needs to be given on the subject of data sharing.
The impacts of Freedom of Information need to be considered.

Question 13.

Comments: No comment

Question 14.

Comments: No comment

Question 15.

Comments: Legal framework is too complicated – there needs to be an ‘idiot’s guide’ drafted alongside the Act and it should be re-written in plainer English. We believe that what constitutes personal data, and the actual definition of personal data should be re-defined with more clarity.

Section 4: Consent and transparency

Question 16.

Comments: We consider that the issue of consent is very unclear. For example, internal staff grievance processes in both public and private sectors are quasi-legal proceedings. There is no provision for the implications re DPA when proceedings are taking place.

Question 17.

Comments: We believe that this would not be practical for the criminal justice arena – and would serve as a disincentive for society. There needs to be clear guidance on consent.

Question 18.

Comments: We consider that there needs to be more clarity on the issue. The individual’s rights need to be strengthened, but balanced accordingly against the purposes and requirements of the criminal justice service.

Question 19.

Comments: We believe that the Framework adds value in a theoretical sense, but needs to give some best practice advice for organisations.
We consider that privacy impact assessments are too theoretical and have not considered the practicalities of what is required. Again, we consider that best practice examples would serve to be a helpful tool is possible.

Section 5: Technology

Question 20.

Comments: Sharing of information has been eased, but we consider that this has increased risks associated with sharing. As mentioned before, we do not consider that the Act has kept pace with advances in technology and needs to be re-written

to reflect this.

Question 21.

Comments: Yes – we believe that there should be a requirement for all holdings of personal data to be encrypted, especially where those organisations have registered with the ICO. We do not think that this would be a good idea when considering where an individual holds only their own personal data – they should safeguard that information to the level they think is appropriate.

Question 22.

Comments: We consider that anonymisation is a useful tool, and the CPS regularly uses this method when data sharing for non-specified purposes is necessary.

Section 6: International comparisons

Question 23.

Comments: We are aware that the French Data Protection Act exempts all criminal case information.

Question 24.

Comments: No

Question 25.

Comments: No

Question 26.

Comments: Yes – in the USA where Freedom of Information rules supersede privacy laws.

Section 7: Additional questions

Question 27.

Comments: Yes – we consider that one off data sharing protocols on a sector level should be considered.

Question 28.

Comments: We believe that there should be a consolidated Information Act (incorporating Freedom of Information and Data Protection Act in one).