



Information Commissioner's Office

The Information Commissioner's response to the Welsh Government's Consultation on the Proposals for Legislation on Organ and Tissue Donation: A Welsh Government White Paper

The Information Commissioner's Office (ICO) is the UK's independent public body set up to promote access to official information and the protection of personal information. We have responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000. We do this by providing guidance to individuals and organisations, solving problems wherever possible, and taking appropriate action when the law is broken. The ICO will provide responses to questions relevant to the scope of this office, and from the perspective of the Data Protection Act. Responses have been provided to questions 5, 7 and 9 only.

The Data Protection Act ("DPA") relates to the handling of the personal information of living individuals only; it does not cover that of individuals once they are deceased. Our response to this consultation therefore relates only to the handling of the consent data of individuals while they are living.

Anyone who processes personal information must comply with the eight principles of the Data Protection Act, which make sure that personal information is:-

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with the individual's rights
7. Kept secure
8. Not transferred to other countries without adequate protection

Question 5 – In relation to the record keeping options for the soft opt-out system –

a) Which of the suggested options do you prefer?

From the perspective of data protection, there are issues and benefits associated with all four of the proposed options. Whichever option is ultimately selected, we would seek assurance that the data protection implications are considered in full by the Welsh Government, to ensure compliance with the eight principles of the DPA (above). We hope that a full consideration of the privacy implications of the selected option will be made during the privacy impact assessment which has been scheduled to follow this consultation process.

In our view, the main considerations in selecting one of the four options are around the relevance and quantity of the personal information held, and its accuracy and security. **Option A** would involve the operation of three separate registers (including the existing ODR), which would raise concerns around the relevance of the personal data being processed, whether the personal data being processed is excessive, and how the accuracy of all of the registers could be maintained so that they are consistent with each other, and of course the processing of larger volumes of personal data would mean a greater security risk. However Option A is in our view the one which would be likely to provide the greatest reassurance around data accuracy, as it is arguably the one which gives the greatest clarity around the individual's position and would enable the most accurate and up-to-date recording of his choices, as presumably one register could act as a cross-check of the other.

Option B involves the maintenance of one register alongside the ODR. Since this 'extra' register would capture all those who have not objected, this means in effect a register of the entire (eligible) population in Wales in the first instance, until objections start to be received and individuals' details can be removed from the register. There would be no way of cross-checking to ensure the accuracy of the register as there would be under Option A. In our view, this option also raises concerns around administration; how would the audit trail reflect that an objection had been received and actioned? If there is no register to record objections, would this mean that objections would need to be kept in a separate place once a name is deleted from the register? We would most certainly advise against the records of objections being deleted entirely.

Option C is the best option from our perspective in terms of data minimisation; that is, ensuring that the amount of personal data being handled is kept to a minimum. The less data that is held by an organisation, the less chance of something going wrong. In addition, personal data that is collected and processed by an organisation needs to

be 'relevant' for the purpose, and so an organisation should be able to justify its processing of any piece of personal data. Only those voicing an objection would be captured on the 'extra' register. It would also solve the problem identified in Option B around audit trails. However, there are other data protection considerations – particularly in terms of data adequacy and relevance. Care would need to be taken that enough (but not too much) identifying information is captured for any individual making an objection, to ensure that in the event of their death, the database is consulted and the correct individual identified. For example, there could be serious repercussions or significant distress if an individual with the same name had objected, but the wrong family was consulted, and such an occurrence would also impact negatively on public trust in the system. As with Option B, there would be no apparent cross-check of data to assist with accuracy.

In our view, **Option D** raises similar concerns to Option C. Option D would certainly assist with data minimisation, in that less data would need to be held, and it could have an inbuilt accuracy check via GPs to ensure that records were always up to date. However, there would be issues around consistency, and ensuring that all members of the public are afforded the same opportunities to object, and that any objections are handled the same way; this would be more difficult to manage if responsibility were delegated to individual GPs. There may also be complications in identifying who the actual data controller is, particularly for individuals seeking to exercise their rights under the DPA. There is also the question of how the system would handle those who for whatever reason are not registered with a GP. In our experience, a lack of centralised control can be a recipe for problems.

From a data protection point of view, therefore, the ICO's view would tend towards option A or C. Whilst there would still be data protection issues to be addressed, option A would appear the best in terms of data accuracy, and option C seems to be the best way in terms of minimising the amount of data held, while still providing for accuracy. However, whichever option is finally selected, we would expect that full consideration is made of the data protection and privacy implications. It would only take one instance of an incorrect decision being made as a result of the holding of incorrect data in order to bring the whole system into disrepute. The Information Commissioner now has powers to fine up to £500,000 for breaches of the DPA such as this, however we consider that the loss of reputation and public trust would be likely to prove of greater consequence than any financial cost.

Finally, whatever option is finally decided upon, as mentioned above, it will need to include an adequate mechanism for recording an individual's change of mind. It would also need to have provision for ensuring that individuals' other rights under the Act are respected, such as the 'subject

access right', which allows (with some exceptions) individuals to have a copy of all information that is held on them.

b) Are there other options you feel would provide an effective and secure system?

We have no specific alternative options to recommend, but would again reiterate the importance of ensuring the compliance of any selected system with the eight data protection principles. We note the suggestion on page 12 of the consultation, in respect of the potential for the existing ODR to be adapted to accommodate the new soft opt-out system. In our view, adapting the existing system would allow the Welsh Government to benefit from established security and accuracy measures. Maintaining one system would decrease the security risk that would occur as a result of operating two, or even three, entirely separate registers in (potentially) different ways.

Question 7 – How can the Welsh Government ensure that the public awareness campaign is effective?

We welcome the Welsh Government's intention to publicise the soft opt-out system widely, to ensure that everyone in Wales who would be affected by this change will be fully aware of the system and the process for making an objection.

The first data protection principle says that personal information must be processed fairly and lawfully. One of the requirements of the first principle, to make any processing fair, is to provide individuals with what is sometimes referred to as "fair processing information". This means providing members of the public with information such as who will be holding their data and why, how it will be held, and what will happen to it.

Therefore, we would advise that any awareness campaigns should include this information as a minimum. We also consider that the public should be made aware of the role of any third party (such as a contractor) that may be involved in processing their data, and – of course – the process for making an objection. We would expect that consideration of these issues would form a part of the Welsh Government's privacy impact assessment for the proposal.

We would also advise that consideration be given to ensuring that the awareness campaign reaches all of Welsh society, taking account of all sectors and communities; to ensure that the processing is "fair" for everyone and that all are fully informed. Every effort should be made to ensure that each individual affected will know exactly where and how

their information will be held, and they will know exactly how to make an objection to the processing.

The Welsh Government should not underestimate the work that would be entailed in order to achieve an effective awareness campaign. We have commented in the section below on the term "presumed consent". In our view the ideal benchmark for public awareness should be 'fully informed' rather than any 'presumption' of understanding.

Question 9 – The Welsh Government has asked a number of specific questions; if you have any related issues which have not been specifically addressed, please record them here.

We have touched on some of the requirements of the DPA within our specific responses above, but the issues we have raised are not, by any means, exhaustive. Further general guidance is set out below. In accordance with our role of providing advice on the application of the Acts we regulate, we would also be happy to assist with any further advice and guidance that may be required.

1. Sensitive personal data

Any of the proposals included in the White Paper would involve the processing (i.e. the collection and storage at the very least) of the personal data of many individuals. Information relating to the physical or mental health, or physical or mental condition of any individual falls within the DPA's definition of "sensitive" personal data. This type of information requires an even more solid basis for processing, due to the level of detriment if something were to go wrong. This includes a likely requirement to obtain the *explicit* consent of all individuals, which could have significant implications for the current proposals. Whilst preparing our response to this consultation, we considered whether the personal data (i.e. individuals' wishes relating to organ donation) would fall within the definition of "sensitive" personal data, and came to the conclusion that this information would not be defined as "sensitive".

The reason for our conclusion is because even though the information collected would be intended for future use in a medical context, ie in the event of an individual's death, whilst they are still alive the act of collecting and storing someone's wishes in regard to consent amounts simply to recording an expressed view. We do not consider that this could be classed as information relating to physical or mental health, as in the above definition of sensitive data.

If on the other hand there is any intention whatsoever of storing at any time information relating to a person's physical or mental condition alongside their consent wishes, for example, noting defective eyesight or

a damaged organ, then explicit consent would be the only way forward. Any other form of consent would be likely to constitute a breach of the Act.

2. Consent terminology

Discussions around consent can be complex, particularly since it has no single definition. The White Paper uses the term “presumed consent”, which – in this context - describes a system that “permits material to be removed from the body of a deceased person [...] unless the person had expressed his or her opposition before death by filing an objection with an identified office or an informed party reports that the deceased definitely voiced an objection to donation” (World Health Organization). We appreciate that the term is the standard one used to describe this kind of system. However, some consider that the notion of “presumed consent” implies an element of action being taken regardless, which can in itself lead to public concern and potential negativity. In the context of handling personal data, the ICO view is that if at all possible, consent should be freely given and able to be retracted, with the individual having been given enough detail to make an informed decision.

If the current proposal goes ahead, the Welsh Government may want to reconsider how it uses the term “presumed consent”, and in the context of communicating with the general public to emphasise its commitment to a standard of ‘fully informed’ rather than to any presumption of understanding. If this was done properly it would lead to the public effectively being able to give their informed consent, even if technically they do not need to positively signify that consent (ie by ‘opting-in’).

3. Contractors (Data Processors)

The consultation document points out that the current ODR is maintained and held by NHS Blood and Transplant, but of course it is not yet clear who might act as data controller for any new register implemented to administer the soft opt-out system. It may be that, if a third party organisation holds and maintains any new register on behalf of the identified data controller, there could be a data controller-data processor relationship. At that point we would advise that full consideration be given to this, to ensure compliance with the information security requirements of the DPA; through a written contract, and appropriate security controls being included in that contract.

4. Accurate recording of consent

We understand that however the soft opt-out system is administered, it is likely to mean the introduction of a new register that captures the personal data of a large number of individuals. There is no suggestion as

yet as to what data would need to be collected for each individual, and this may depend on the option that is selected. In terms of the requirements of the DPA, the amount of information captured should be sufficient to ensure accuracy on the one hand (and therefore comply with the fourth DPA principle) but not enough that it becomes excessive and lacks relevance for the purposes of administering the soft opt-out system (therefore complying with the third principle).

It is hoped that this response provides a clear statement of the ICO's position on this matter. We would of course be pleased to discuss or expand further upon any of the points raised above.

January 2012