Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to Ofgem's consultation on the priority services register review - final proposals

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003.

The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. He does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The DPA governs how organisations handle personal data, setting rules in respect of how it is processed (stored, held, used, collected and any other activities), the information to be shared with data subjects about that processing and the security of that data, amongst others. As well as personal data (data relating to living individuals, which identifies those individuals), the DPA also defines a further category of 'sensitive personal data' (information about a person's mental or physical health, ethnicity or race amongst other things) with an expectation of higher protection for that sensitive data. Data about individuals' medical conditions – such as the need for a respirator or kidney dialysis equipment as referred to in the draft 'needs' codes would be sensitive personal data for the purposes of the DPA.

The Commissioner welcomes the opportunity to respond to this consultation on Ofgem's final proposals relating to the review of the existing Priority Services Register (PSR) in the gas and electricity sector. We recognise the importance of having this resource, so that energy companies can ensure those with particular vulnerabilities are identified and ensure that appropriate provision is made to maintain continuity of service and to assist those individuals.

We have followed the review of the Priority Services Register provisions with interest, having responded to the earlier consultation and subsequently had some contact with the Customer Safeguarding Working Group in the early stages of drafting the cross-sector 'needs' codes. We support the scheme's aims but are keen that those involved ensure it is

implemented in a practical and compliant way with minimal exposure to individuals' sensitive personal data. We remain happy to provide input and advice on data protection issues if needed.

We have only responded to those questions within the consultation that are relevant to the Commissioner's regulatory role.

Question 1: Do you agree with our final proposals for enhancing eligibility and customer identification and the associated proposed licence conditions?

Enabling suppliers, Distribution Network Operators (DNOs) and Gas Distribution Networks (GDNs) to reflect customer circumstances and needs more accurately can only be a positive thing. This is particularly the case where any changes enable less detailed or sensitive information to be held and/or shared than would otherwise have been required.

If the intention is to encompass more transient vulnerabilities, then it is important that regular review of the information recorded about individuals' vulnerable situations and/or vulnerabilities is built in from the outset.

The DPA obliges organisations to keep the personal data that they are processing accurate and up to date, as well as adequate, relevant and not excessive for the purposes that it is being processed for.

In addition to those obligations, we would like to see the licence conditions include an obligation to keep information about customer vulnerabilities under review. The potential for additional enforcement (by Ofgem, in addition to the ICO) would provide reassurance to individuals when handing over their sensitive personal data and give an appropriately robust message to the organisations involved.

Question 3: Do you agree with our final proposals for recording and sharing information about customers in vulnerable situations and the associated proposed licence conditions?

Review

In terms of recording information about customers' vulnerabilities, reference is made within the consultation document to a need to periodically review that information. As mentioned earlier in our response, we would like to see this obligation reflected within the amended licence conditions to ensure that the obligation to review is sufficiently embedded in the process.

Customer consent

A number of references are made within this section to obtaining, holding and sharing personal data with customer consent. To comply with the DPA, a fundamental requirement is the need to be able to justify processing of personal data in line with one of the conditions for processing specified within the DPA. One of the available conditions is consent. However, there is a risk to over-reliance on consent as a justification for processing under the DPA. Consent (a freely given, specific and informed indication of wishes) can inherently be refused or withdrawn. Where information is being processed on the basis of the data subject's consent, you need to be clear on the consequences should that consent be withheld or withdrawn.

To be clear, we are not suggesting that the processing which the suppliers and DNOs/GDNs will be undertaking cannot be done in compliance with the DPA. The point is rather that there may be circumstances where relying on consent to justify that processing may not be possible, and it is important to consider this possibility before it arises in practice.

An example where this might arise might be information which a customer shares in conversation with a supplier indicating a vulnerability, but which that customer does not wish to have recorded by the supplier for whatever reason. If the supplier is relying solely on consent, it would be unable to retain that information, and consequently would struggle to justify retaining it. Suppliers, DNOs and GDNs need to consider what other justifications for processing that they may be able to rely on as an alternative to consent.

We also need to highlight that change is imminent in the UK's data protection landscape. The UK's DPA is based on a European directive, which is due to be replaced in the near future as part of a European-level review of data protection legislation. A new European General Data Protection Regulation (GDPR) has been drafted, and should that be approved by the relevant European institutions, will have direct effect in the UK at the expense of the DPA. In terms of the likelihood of this happening, we are currently awaiting political agreement in Europe, following which a finalised, agreed version will be published in the official journal and a two year countdown to implementation will begin.

The GDPR sets additional requirements for consent – including a requirement that consent be 'unambiguous' and must be indicated via a statement or 'clear affirmative action'. There are also additional expectations that those relying on consent should keep records in terms of obtaining that consent. Given the intended implementation timetables for the proposed data sharing, we would recommend that you follow developments in this area over the coming months to ensure that any arrangements put in place are compliant prospectively.

Developing data sharing arrangements

Central to any data sharing arrangement should be the minimisation of the personal data to be shared, that is, limiting the shared data to the minimum necessary to achieve the intended purpose. In terms of sharing data between organisations, the draft 'needs' codes in Appendix 4 to the consultation raise some questions.

As we set out in our consultation response in September 2014, we strongly agree that there is a need to ensure that any codes used across the sector can be applied consistently or, as a minimum, translate between organisations to ensure a universal understanding is achieved where needed. What is unclear from Appendix 4 is whether the detailed needs codes will be shared between organisations, or whether only the broader categories will be shared. We would recommend that the less detailed information be shared in preference to the detailed to the greatest extent possible, as a way of reducing risk to individuals and their data. The detail included in the individual needs codes is such that it could be subject to serious abuse if not kept appropriately secure.

This is not to say that there will never be circumstances when the sharing of more detailed information is required, but rather that the default should be to share the less detailed categories rather than the detailed need codes wherever possible. Appropriate sharing is based on organisations understanding the motivation for the sharing and not applying blanket rules irrespective of the specifics of the situation.

We would be happy to provide assistance on the data protection implications of sharing personal data between organisations to the Customer Safeguarding Working Group (or other involved parties), if needed. Our guidance on data sharing (https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/) may also be of assistance.

February 2016