The Information Commissioner's response to Ofgem's consultation reviewing the Priority Services Register

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.

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

The Commissioner welcomes the opportunity to respond to this consultation reviewing the existing Priority Services Register (PSR). We recognise the importance of having this resource, so that energy companies can ensure those with particular vulnerabilities are identified and, in the case of emergencies such as the power cuts last winter, ensure that appropriate provision is made to maintain continuity of service and protect those individuals.

The DPA sets eight principles of good information handling, which organisations must follow when collecting, storing, using or otherwise processing individuals' personal data. Information recorded on the PSR (name, address, information about health, abilities, age) is personal data under the DPA and must be treated as such.

These principles include obligations to: let individuals know what their personal data is being used for (known as giving 'fair processing' information); ensure that any data processed is accurate, up to date and relevant for the purpose it is being used for; keep personal data secure; and to only process the data for the purposes it was collected for.

In addition to the requirements for the processing of personal data, where 'sensitive' personal data is processed additional safeguards must be used. 'Sensitive' personal data includes information about an individual's race or ethnic origin, political opinions, religious beliefs, physical or mental health and any actual or alleged criminal background. A supplier maintaining a PSR is likely to be processing sensitive personal data.

We have only responded to those questions that engage the remit of the Commissioner as having a data protection or privacy aspect. We take this opportunity to offer Ofgem and the energy companies advice and support in considering the data protection implications of implementing any changes to the existing PSR.

5: Do you agree that energy companies should be required to maintain a wider register of consumers that they have identified as being in a vulnerable situation?

We cannot comment on who should be included within the PSR as that is a decision for the energy companies, Ofgem and any relevant government departments to make.

We want to emphasise, however, that any expansion of the PSR (in terms of scope and/or size) will result in more personal data being processed. In some cases this data will be sensitive personal data for the purposes of the DPA - for example, when the PSR indicates that a customer has a particular medical condition. Any processing of this data (whether sensitive or otherwise) needs to be justified, and steps taken by the organisations collecting, using and sharing this data to ensure that any data processed is accurate, relevant and up to date.

Any system of flags used – whether universally used across all organisations or otherwise – needs to be consistent and the flags need to accurately represent the issue they are being used to address.

6: Do you agree that suppliers, DNOs and GDNs should share information about customers' needs with: (a) each other? (b) other utilities?

Any data sharing needs to be entered into on the basis of an identified, legitimate need. We are not in a position to identify whether there is such a need within the energy sector, but we would expect that the energy companies themselves, in conjunction with Ofgem and potentially relevant consumer protection or advice groups, should be able to do so.

Provided that the information being shared is accurate, relevant and up to date, there would seem to be customer service and societal benefits to sharing this information. That said, it would be for the parties involved to be confident that the requirements of the DPA had been met where any data were shared. Our data sharing code of practice (accessible at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx) provides advice on sharing data in compliance with the requirements of the DPA and may prove helpful to those involved.

7: Should energy companies be required to share information about customers' needs with other fuel suppliers such as LPG, heating oil distributors. How could the transfer of this information work? What are the benefits and risks of sharing the information?

Again, we would not comment on whether the data 'should' be shared with the wider fuel supplier community. Any such sharing needs to be considered from the perspective of what is necessary in the circumstances. For example, it would be difficult to justify sharing data of *all* customers on the PSR with other fuel suppliers if only a minority are likely to use such fuels – such sharing would result in those alternative fuel suppliers processing significantly more personal data than they have a need to. However, sharing the data of those who are known to use those fuels would be easier to justify as having an identifiable benefit. Any requirement to be placed on suppliers needs to enable the context to be considered, rather than being an indiscriminate rule which applies across the board and does not enable relevant contextual factors to be taken into account.

It is important that organisations sharing data understand what data they are sharing and for what purpose. This should help ensure that the data shared is adequate, relevant and not excessive
in compliance with principle 3 of the DPA. Organisations also need to be able to ensure that any data shared for this purpose is 'ringfenced' and only used for this purpose to avoid unfairness arising.

We would recommend that organisations look to the data sharing advice contained within our data sharing code of practice (available online at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx).

Organisations considering embarking on a new data sharing project might also find it helpful to carry out a privacy impact assessment (PIA) to work through any privacy and data protection issues relating to that data sharing. Our PIA code of practice details how to undertake a PIA (available online at: http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf).

8: Do you agree that we should stipulate the maximum details that we expect energy companies to share, for example that names and phone numbers must be shared when they are

available? Is there any other information that should be shared and for what purposes?

It is for the organisations involved (Ofgem and the energy companies) to establish what data needs to be shared and to be clear on why that specific data needs to be shared. Each category of information needs careful consideration to determine justification and data should not be shared on a 'just in case' basis. The advantage of having an agreed position common to all parties (provided that it takes into account organisations' needs) is that the agree position removes the need for each organisation to separately and repeatedly determine whether data should be shared on a 'case by case' basis. This should result in a more consistent approach to data sharing.

We would also point out that, depending on the circumstances in which the sharing is taking place, it may be necessary to have more than one agreed sharing standard. Again, the organisations involved need to establish what information may be required in different situations and work towards those standards.

9: Do you agree that energy companies should agree common minimum 'needs codes' to facilitate the sharing of information? Should we require energy companies to agree these codes? How might this work and what mechanisms are already in place to facilitate this? What role would Ofgem need to have in this process?

The DPA does not require that personal data is only shared subject to agreed codes, however, having a universal set of codes would be a sensible approach if it can be reasonably facilitated by the organisations involved. Compatibility with existing systems is something which would need to be carefully considered when deciding whether or not to introduce universal codes.

Any such codes, if agreed, would need to be accompanied by instructions for use to ensure that they are consistently applied across different organisations. The key point is to ensure that any such codes do not result in organisations processing inaccurate personal data about individuals, as a result of different understanding or application of the codes used.

The nature of any agreed codes needs to be carefully considered – that is, whether it is more effective to choose codes to reflect the individual's vulnerability or adjustment required (for example, a customer's inability to communicate via telephone) or whether the code should reflect any condition the individual has (for example, deafness or a speech impediment). There are potential benefits and pitfalls to both

approaches. From a purely practical perspective, recording the customer's adjustment or vulnerability could act to reduce the recording of excessive or particularly intrusive (sensitive) personal data. We recognise, however, that this may run contrary to systems in place in the industry and cause significant practical issues. A negative of adopting this pragmatic approach is that it might reduce organisations' ability to recognise where further services might be needed by a customer which recording information about a customer's specific condition might facilitate.

Whichever route is adopted, we would recommend careful consideration of all the possible consequences of both courses of action by working through a PIA.

10: Should information about a customer's needs be shared with their new supplier when they switch? What is the best way to facilitate the sharing of this information?

From a DPA perspective, customers need to be aware of how their information is being used. When customers register any priority services with an energy supplier, there would be an opportunity to let those customers know how that particular priority service information would be used – including any sharing of that data. Additionally, at the point at which a customer chooses a new energy supplier that supplier would also have an opportunity to inform customers of any necessary data sharing. If, however, customers have not previously been notified of the data sharing, it would be simplest for customer consent to be obtained at the point of switching services.

However the sharing takes place customers either need to have been notified of that potential sharing at the time the relevant data was collected, or to have consented to that sharing of data. This is particularly the case where a customer's vulnerability (or the household's need for priority services) may be transient or temporary - for example, if a relative with energy-based medical needs moves in for a short period of time. Thought would need to be given to how the information can best be kept accurate and up-to-date. Even if the information has been legitimately shared between old and new suppliers, it may be appropriate for the receiving supplier to confirm the information to ensure its accuracy.

If data is to be shared between different energy suppliers, the importance of ensuring that the information in question is accurate and up-to-date is even more important. A universal codes system would be valuable where information is to be shared in this way, removing the potential for inconsistencies and misunderstandings between organisations.

11: Do you agree that a single cross-industry brand will raise awareness of priority services?

This is not specifically a data protection or privacy issue. However common sense would suggest that a coordinated approach across energy and water industries – and the creation of a single brand - might help to remove any confusion as to what services are available and who those services are available to.

12: Do you agree that a guidance document would help advice suppliers and raise awareness? Who should produce this document?

As with a single brand, it may be that a central guidance document would help raise awareness. Any document created needs to be accessible in formats appropriate for the vulnerabilities it is intending to address – to acknowledge the differing audiences of advice suppliers and services users. The accessibility and ready availability of any such guidance would also be crucial.

13: What more can be done to raise awareness of priority services?

This is not specifically a data protection or privacy issue. However common sense would suggest that a coordinated approach across energy and water industries – and the creation of a single brand - might remove any confusion. Similarly, a set of common minimum services might help ensure consumers are clear on what help is available and in what circumstances.

14: Do you agree that supplier independent audits are the best way of monitoring companies' compliance with our proposed obligations? Do you have views on the approach that audit should take and what it should cover?

The proposed changes seem to take better account of assessing the effectiveness of the overall scheme in comparison to the existing approach. If audits are able to factor in not only the volumes of customers covered on the PSR but also the accuracy of the information recorded and used, then that would seem a better reflection of the state of the PSR.