The Information Commissioner's response to the Department for Energy and Climate Change's consultation on proposals to amend domestic energy supply licence conditions - requiring provision of key energy data in a machine readable format

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). 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 Information Commissioner welcomes the opportunity to respond to the Department for Energy and Climate Change's (DECC's) consultation on proposals to amend domestic energy supply licence conditions to require provision of key energy data in a machine readable format.

We understand the Government's intention is to improve the consumer experience in the energy markets by making the switching process quicker and easier. We note this consultation is to inform licence modifications that would require suppliers to place key customer energy data in machine readable format on energy bills, benefiting consumers by enabling them to compare tariffs and secure the best energy deals.

We support proposals that empower consumers by providing them with more information to enable them to make better informed decisions, and we have had involvement in early development stages of the Government's midata project. Whilst we agree broadly with the requirement to provide energy data in machine readable format and agree it is essential that consumer's data is safeguarded, we have identified some potential data protection concerns which need to be addressed.

Our concerns relate to how much personal data will be accessible when providing the consumer with their data in machine readable format. It is important to carefully consider how much, and specifically what, data is accessible and to ensure this does not expose individuals to unnecessary

risk. It is also important to carefully consider the security of any data accessible and ensure appropriate steps have been taken to protect the data from unauthorised or unlawful access.

If the information accessible in machine readable format is what is already on the paper bill (but perhaps set out in a format which is more easily understood or easy to compare), and the code to access that format of information is on the bill itself, then we would have less concern given that anyone who has access to the paper bill will already have access to that data.

However, if the information accessible differs significantly in volume, detail or content (perhaps information that could only be accessed under normal circumstances by contacting the energy supplier and going through security procedures and identity verification), then this would be more of a concern. We would also be concerned if more detailed or sensitive information could be easily accessed, for example by simply scanning a QR code, without the level of security and identification checks that would be required if the same information was accessed by different means.

It will also be relevant to consider the visibility of the QR code to third-parties. For example, ensuring it is not visible through the envelope address window or printed on an external face.

There is a pressing need to ensure that the use of QR codes is implemented in a privacy friendly manner and that data protection is considered from the outset (a 'privacy by design' approach). We recommend that a Privacy Impact Assessment (PIA) is undertaken in order to assess the risks arising from the release of data in machine readable formats; our recently updated Privacy Impact Assessment Code of Practice sets out the principles for carrying out a PIA. A PIA is a useful means by which to identify and evaluate privacy risks, and should help to identify ways in which those risks can be eliminated or managed at an early stage.

We acknowledge that the Department for Business and Industry's feasibility study into the use of QR codes indicated that the risk of data abuse was minimal, however we note the study did not undertake to explore in full all potential data protection issues. We also note the study recommends that data protection is an area for expert advice during any subsequent detailed solution specification. We would therefore like to offer our assistance to DECC in discussing data protection in more detail as these proposals develop.

Below we have responded to the consultation questions which have an information rights aspect.

Question 3: Do you agree with the proposed text for the 'call to action'; if not please propose amendments together with your rationale for them?

When customers are presented with their bills or statements containing this new machine readable information, it is important that they are given clear information as to how it works, who is holding their information and what will happen with their information. The first principle of the DPA requires individuals to be informed as to how their information will be processed and you would need to ensure this requirement has been met through the provision of sufficient information to the consumer.

Question 4: Are there communications other than bills or statements of account on which it would be useful to include key customer data in a machine readable format?

There are a number of ways in which technology such as QR codes could potentially be misused or manipulated. A real-life example was where QR codes were included on parking meters to direct smartphone users to an online payment portal. A third party created fraudulent QR codes which they placed over the originals, resulting in individuals being directed to unrelated third-party sites which took payment.

Limiting the use of QR codes to direct communications between the energy supplier and the individual customer should make some of these types of scam more difficult – as to substitute the code would involve intervention at source or wholesale spoofing of bills and account information. When considering the inclusion of QR codes on more generic leaflets or other communications it is worth considering what level of control the energy supplier has over that communication and therefore whether this could introduce vulnerabilities into the process.

Question 7: Should the licence modifications limit the range of machine readable formats, for example to those that have data embedded in them and, if so, should we prescribe the minimum image size (2x2cm) of such images?

It is our understanding that there are two broad approaches which could be adopted: where data is embedded within the QR code itself or where a unique identifier is used which links to this same data in an online database. Either of these approaches could also be incorporated into a URL to direct users to an energy provider's website or read by a third-party app and used for price comparison. In respect of this we have some concerns about whether the former approach will feasibly fit within consultation's preferred smaller sized QR codes (e.g. a 2cm by 2cm QR code can contain only about 60 characters). As a result this may cause

the latter approach to be more widely adopted, perhaps by use of a short form URL and unique customer identifier. In this scenario it would be important to ensure an 'attacker' would not be able to guess the identifier in the URL and therefore access the consumer's details by cycling through all possible identifiers.

Question 8: Are there any specific data protection issues relating to trusted third sector advocates utilising machine readable images to inform cross market comparison applications?
Question 9: If so, what safeguards, if any, can be put in place to ensure data, once used, is not retained in an application?

We would expect any third sector advocate looking to develop applications capable of utilising this machine readable information to process personal information in compliance with the DPA. Our recent guidance entitled 'Privacy in mobile apps: guidance for app developers' may be useful for any such potential developments of cross market comparison applications.

In principle we are supportive of the requirement to provide consumers with their information in machine readable format, provided this is implemented in a privacy friendly manner in compliance with the DPA. We would be happy to work with DECC to address any data protection issues identified.