The Information Commissioner's response to DECC'S consultation on New Smart Energy Code Content (Stage 4) and consequential/associated changes to licence conditions

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 on stage 4 of the Smart Energy Code. Data protection and privacy issues impact upon aspects of the proposed framework and we therefore offer our ongoing support to DECC on those matters falling within our remit.

As a general point we would highlight the importance of making sure consumers understand what is happening with their data and what their options are (where personal data is being processed, this is known as giving 'fair processing' information). Smart metering is a complex area and those involved seem to be taking many positive steps to try and make it privacy-friendly – but need to be sure to communicate those choices to consumers in an accessible way.

In responding to this consultation we have only answered those questions that engage the remit of the Commissioner. In particular, we have not commented on the proposed legal drafting referenced in any of the questions we are responding to.

Privacy audit

Q16 Do you agree with our proposed approach and legal text for SEC in relation to Privacy Assessments?

We understand that the proposed approach involves the same centralised body providing both security and privacy assurance assessments. These assessments will include formal assessments at staged points and random sampling. We agree that there is synergy between the two processes and

also that having a centralised body should result in consistent standards being applied across the board.

The important point is that whatever framework is put in place it should be practical, achievable, sustainable, promote privacy friendly practices and ensure the security of consumers' data.

Q17 Do you agree with the specific proposals for undertaking random sample compliance assessments?
Provided that the sampling in question is genuinely random, this should prove a useful additional safeguard for consumers' data.

Q18 Do you agree with the proposal for Users to meet the costs of the privacy assessments that are undertaken at their organisation?
The allocation of costs is not directly a data protection issue. We do however recognise that requiring organisations to pay for their own individual assessments should incentivise those organisations to ensure that they take the process seriously – thereby avoiding further cost implications. Although we understand that cost implications carry a significant weight in their own right, we would hope that other potential concerns (such as reputational damage or even the possibility of not being able to participate further in the smart metering programme) will also assist in ensuring that privacy and security aspects are taken seriously.

Q19 What are your views on potential future changes to the SEC to provide for reporting the results of privacy assurance assessment bodies such as Ofgem, DECC, ICO and Parties generally?
We can see that the reporting of audit results to external organisations, such as the ICO, could help ensure that the auditing operates in a transparent way and in consequence have a positive effect on the reputation of smart metering in general. Such a system could also enable regulators to take a coordinated approach if problems are discovered.

We would not expect to receive copies of all audits or assessments carried out under these provisions. We would, however, be interested in receiving summary information should the auditors identify any significant data protection concerns. The kind of information we might be interested in would be evidence that organisations were disclosing data without appropriate authority, information about significant security flaws endangering personal data or information showing organisations were using data in intrusive ways which individuals had not previously been informed about.

This information would be received and recorded by the ICO as intelligence, and might then be used to inform the activities of our Strategic Liaison, Enforcement or Good Practice teams. We use the intelligence we collect to build a broader picture of organisations' and sectors' privacy and data protection practices, which in itself can form the basis for different ICO activities. For example, where we identify concerns with the way in which an organisation (or sector) is handling personal data, we could choose to formally require further information from that organisation, liaise with that organisation, or look to instigate more formal enforcement action in the most serious of cases. Our enforcement powers range from the ability to require information via an Information Notice, to the ability to require organisations to take certain actions in respect of personal data they hold (via an Enforcement Notice), to the ability in the most severe of cases to issue a Civil Monetary Penalty of up to £500,000. More information about our enforcement powers and how we use them is available on our website at: http://ico.org.uk/what_we_cover/taking_action/dp_pecr and in our regulatory action policy: http://ico.org.uk/what_we_cover/taking_action/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-protection-regulatory-action-policy.pdf.

Consumer consent for connecting consumer devices

Q20 Do you agree that the proposed legal drafting reflects the position reached in the SMETS2 consultation response, that Users should be required to obtain consent and to verify the identity of the energy consumer from whom they have obtained the consent prior to pairing a CAD?

We understand that this change relates to how consumer access devices (CADs) can connect to the smart metering system via the Home Area Network (HAN) – known as remote CAD pairing. Consumers cannot connect additional CADs to the HAN/smart metering system themselves, but must do so via certain DCC Users. CADs will be able to access consumption and tariff data, which we understand could cumulatively be quite informative about a consumer's activities. CADs may enable the viewing of consumption and tariff data, cloud storage of such data or the use of such data to target energy efficiency improvements.

The proposal is that any time a CAD is remotely paired to the smart metering system, the consumer's consent will be required (currently the proposal is that consent is required only in more limited circumstances).

Provided that this measure does not result in consumers being bombarded with consent requests (it is not clear from the consultation how often such pairing might be required or whether it could ever legitimately be required at the instigation of someone other than the consumer), this seems to be a privacy-respecting approach and should

also enable the consumer to stay in control of access and potentially also to identify any unexpected access.

Service to allow consumers to find out which users have accessed their consumption data

Q38 Do you agree with the proposed approach and legal drafting in facilitating provision of a service to consumers to allow them to find out which Users have accessed consumption data from their meters?

This proposal (to enable consumers to see which organisations have accessed their consumption data – the check would be against the service log which records all organisations' requests to access consumption data) is positive from a transparency perspective. It should give individuals an additional level of comfort that they are able to identify the organisations that have accessed their data, and gives them an opportunity to hold those organisations accountable if the access that has occurred is not justified.

This obligation goes further than the DPA would strictly require – via the right of subject access an individual is entitled to know which recipients or classes of recipients have received their data – but this would not usually be an exhaustive list by organisation name. We see this additional transparency measure as a commitment to protecting individuals' smart metering data. It is also positive that the obligation on those wishing to access the consumption data is reinforced with an audit function.