



Margaret Coaster
Smart Metering Team, Ofgem E-Serve
9 Millbank
London
SW1P 3GE

8 October 2010

Dear Margaret,

Response to Smart Metering Implementation Plan Prospectus

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). He is independent from government and promotes access to official information and the protection of personal information. 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 comment on the Smart Metering Implementation Plan Prospectus. Many of the questions in the Consultation Paper are clearly ones which it would be inappropriate for the Information Commissioner to address. For example, some are directed at suppliers, others at meter manufacturers. Therefore, rather than addressing all the questions asked, the following comments are aimed at ensuring that the outcome of the consultation exercise is one which enhances the protection afforded to personal data; in view of this we have not replied to the list of questions in the Prospectus for our response as a number of these are not directly connected with data protection or extend beyond our areas of expertise.

Our comments are based on the Smart Metering Implementation Programme Prospectus and the Data Privacy and Security Supporting Document (Ref 94e/10).

Accelerated rollout

The Information Commissioner acknowledges the advantages of industry being urged to realise more ambitious but achievable targets, but we would urge that this should not lead to rushed decisions that fail to embed data privacy into the framework for smart metering.

One of the Commissioner's chief concerns would be that in the event of a quicker rollout it may be tempting to take shortcuts that would bypass the data privacy and security features that need to be embedded into the plans for the rollout. In any revisions to recommendations, it is crucial that the same thoroughness demonstrated so far in terms



of handling personal data continues. If it is necessary for plans or suppliers or technical specifications to change as a result of the acceleration, then the models of good practice need to be able to fit. It would be unacceptable for the security of personal data to be compromised in the interests of meeting demanding timescales.

So far, much attention has rightly been given to the customer experience and the key role that this plays in achieving a successful rollout. If the rollout were to be accelerated, it would be essential to ensure that factors affecting the consumer perspective were not hurried. Undue haste could potentially lead to mistrust and uncertainty, clouding the advantages that smart metering may bring in terms of energy savings and customer choice and so on. Consumers must be confident about the security of personal data and understand how it will be used; in other words, the message must be transparent and systems properly designed and tested in order for consumers to be convinced.

Privacy by Design has been recognised internationally as a standard for data protection good practice. Having already conducted a Privacy Impact Assessment as part of this project at an early stage has demonstrated the commitment to embedding privacy into project design. Where any design changes are made to accommodate revised timescales, then a Privacy Impact Assessment should be systematically applied in order to ensure that the security of personal data continues to be embedded and serious problems are avoided in the future.

Consumer interests

Naturally, the Information Commissioner supports consumer privacy interests being given prominence and recognises the emphasis that has been placed on this so far. Data privacy is inter-related with delivering a fair and transparent service to the consumer. The Commissioner would be pleased to continue to liaise with Ofgem in preparation for introducing its package of measures in Spring 2011 to provide for the continued safeguarding of consumers' interests.

Whilst the Commissioner would cautiously support the principle that consumers should be able to choose how their own consumption data is used and by whom, the home area network would need to have rigorous safeguards in place and customers must be made fully aware of the implications of releasing their data and to whom they are releasing it. Given that there will be complex inter-relationships in the infrastructure supporting smart metering, which are likely to escalate dramatically once the smart grid reaches its full potential, it is vital that good practice safeguarding individuals is embedded from these very early stages.

The Information Commissioner understands that suppliers will be able to use consumption data in sophisticated ways to offer their customers better energy efficiency products and advisory services. Handled properly, this can be a significant tangible



benefit for the consumer. The second principle of the Data Protection Act 1998 (DPA98) states that personal data shall not be processed in any manner incompatible with purposes specified by the data controller. The escalation in volumes of personal data that smart metering brings creates new opportunities that will, understandably, be attractive to suppliers or third parties. All participants will need to understand their obligations to the DPA98 and work within its boundaries so that their processing of personal data does not stray from its specified and lawful purpose and beyond consumers' reasonable expectations.

The Information Commissioner would agree that meters should be designed so that customers can readily access information available from them. There should be convenient and secure methods for sharing information with third parties when consumers so choose, for example, when they want to receive advice about energy efficiency. However, it is of absolute importance that the consumer must be fully aware of the consequences of doing this and whom they should contact if the need arises. Security checks must be in place so that data from meters can only be accessed by those who are entitled to do so. Furthermore, a process should be established so that any applications which use data from meters need to be checked and certified or approved in order to prevent excessive data collection, security breaches or incompatibilities.

Personal or aggregated data

It will be insightful to have a clearer picture from industry participants about the extent to which they will need to handle personal data (remembering that this includes data that can be linked back to an individual rather than that which directly identifies the customer). Processes become much simpler when data can be anonymised, and the Commissioner would recommend that this occurs wherever possible. Furthermore, where personal data is being processed, it should be kept to a minimum, retaining only that which is necessary to achieve specified purposes. Retaining personal data *just in case* it might be useful in the future is not a justifiable reason for retention.

Privacy Policy

The Information Commissioner would welcome the implementation of an over-arching privacy policy for smart metering. In order to maximise its effectiveness and consistency, we would envisage that the best approach would be some kind of code containing principles that mirror and particularise data protection principles to all involved. Applied correctly, this would be a vital component in ensuring that smart metering complies with the fairness principle of the DPA98 as it would make the process more accessible and transparent to consumers. The Commissioner would be pleased to lend his advice as necessary.



Data Controllers and responsibilities

The establishment of a privacy policy would require decision making about roles and responsibilities. This is a crucial aspect of smart metering implementation and one that has not yet been fully tackled, presumably because decisions about the smart metering infrastructure have not yet been made. If the DataCommsCo is adopted, then decisions will need to be made about its role in terms of data protection responsibilities and the network of processing relationships with which it will connect. This should be addressed promptly regardless of whether a full or a staged implementation strategy is adopted as part of the revised timescales. These issues should be addressed during early stages as part of privacy impact assessment methodology. Clear data controller responsibilities must be assigned and this should be clearly communicated to consumers. Without clarity over which organisation is responsible for compliance with the DPA98, it will be difficult to ensure that the privacy risks arising out of non-compliance are mitigated.

Question 9 from chapter 3 of the Prospectus invites comments on whether the proposal that the scope of activities of a central data and communications function should be limited initially to those functions that are essential for effective transfer of smart data, such as data access and scheduled data retrieval. The Information Commissioner's view would be that this coincides with his recommendation that personal data processing should not be excessive. Decisions will have to be made about whether the DCC will perform limited functions with other parties carrying out other activities. Whatever decisions are made, the data controller responsibilities must be clearly established at an early stage so that the rights of data subjects are respected.

Security

Throughout the planning and implementation, there must be absolute certainty about security implications for personal data so that unauthorised processing is prevented.

The Future

The arrival of the Smart Grid will clearly bring with it numerous possibilities in terms of energy management, some of which can be anticipated and some of which cannot at this stage. In these early planning stages, principles should be embedded that ensure that systems and processes for personal data do not go beyond that which is lawful, reasonable and fair. The capacity to offer sufficient flexibility to accommodate future requirements and safeguarding data privacy need not be conflicting requirements. Again adopting the Privacy by Design approach, time invested in doing this correctly now, and creating a sensible balance is likely to save potentially huge disruption in the future. It is just as relevant to foresee privacy implications as it is to anticipate commercial



opportunities or plan the technology. It is essential that systems designed now are able to ensure that future developments do not conflict with current or future privacy concerns.

Yours faithfully,

A black rectangular redaction box covering the signature of the official.

On behalf of the Information Commissioner's Office