Department of Energy & Climate Change

Smart Metering Implementation Programme

Privacy Impact Assessment

December 2012

Department of Energy and Climate Change
3 Whitehall Place
London
SW1A 2AW

Telephone: 0300 068 4000
Website: www.decc.gov.uk

For further information on this Privacy Impact Assessment, contact:
Smart Metering Implementation Team – Data access and privacy team
Department of Energy and Climate Change
Room 103
55 Whitehall Place
London
SW1A 2AW
Telephone: 0300 068 6996
Email: David.Bull@decc.gsi.gov.uk

The Privacy Impact Assessment can be found on DECC's website:
http://www.decc.gov.uk/en/content/cms/tackling/smart_meters/smart_meters.aspx

Published by the Department of Energy and Climate Change

Document reference: 12D/023 – Smart Metering Implementation Programme – Privacy Impact Assessment

Additional copies:
You may make copies of this document without seeking permission. An electronic version can be found at http://www.decc.gov.uk/en/content/cms/tackling/smart_meters/smart_meters.aspx

Other versions of the document in Braille, large print or audio-cassette are available on request. This includes a Welsh version. Please contact us at the address above to request alternative versions.

Confidentiality and data protection:
Information provided in response to this privacy impact assessment, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004).

Contents

Introduction

The roll-out of smart meters will play an important part in Britain`s transition to a low-carbon economy and help us meet some of the long-term challenges we face in ensuring an affordable, secure and sustainable energy supply.

Smart metering will result in a step change in the volume, granularity and accuracy of energy consumption data that is made available by electricity and gas meters. Consumers will have near-real time information on their energy consumption to help them control energy use, save money and reduce emissions. Suppliers will have access to accurate data for billing and to improve their customer service. Network operators will have better information upon which to manage and plan current activities and the move towards smart grids which support sustainable energy supply. The new opportunities that this data provides in terms of delivery of benefits also raises new questions about the protection of this data and consumers' rights to privacy.

The Government takes privacy issues seriously, and is following international best practice in undertaking Privacy by Design, which means that privacy issues are considered and embedded into the design of the programme from an early stage. We have recently set out requirements for a range of measures for the GB roll-out of smart meters to ensure consumers are protected and any potential privacy impacts are addressed. These requirements can be found in the Government`s response to the consultation on data access and privacy, at http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx#data

The data access and privacy framework will provide clarity about the ways in which energy consumption data from smart meters can be accessed, by whom, for which purposes, and the choices that consumers should have about this. The Government`s response to the data access and privacy consultation sets out the requirements that will be put in place – in licence and in the Smart Energy Code - on all parties with access to data to ensure consumer protection.

Alongside the data access and privacy framework, and in line with best practice, the Government has developed this Privacy Impact Assessment to ensure that as policy has developed, any perceived Privacy impacts have been identified and proposals developed to manage them. The Smart

Metering Implementation Programme has worked on this closely with major stakeholders from the energy industry, consumer groups, regulatory authorities, other external stakeholders and across Government.

In particular, we continue to work closely with the Information Commissioner's Office and the European Data Protection Supervisor (EDPS) on the data access and privacy framework.

Chapter 1 – Overview

Purpose of the document – Why assess privacy impacts?

1.1 Privacy Impact Assessments (PIAs) are intended as a means for organisations to anticipate and manage the potential privacy risks that may arise from policies and programmes. The goal is to ensure that the measures that are implemented minimise privacy impacts and ensure compliance with data protection law.

1.2 Whilst there is no statutory requirement for a PIA to be developed, the Government has chosen to produce a PIA in the interests of best practice. In the Response to Prospectus Consultation the Government said that, as part of its approach to developing a robust privacy policy, it 'recognises the value of carrying out a Privacy Impact Assessment (PIA) to ensure that potential privacy impacts are taken into account in the Government`s technical and governance framework for smart metering'[1].

1.3 This PIA supports an end-to-end 'privacy by design' approach, ensuring privacy considerations are built in from an early stage, and PIAs are recommended as good business practice by the Information Commissioner's Office (ICO). The Government has liaised closely with the ICO throughout the development of this document to ensure that it is fit for purpose. The ICO sets clear guidance on conducting PIAs[2].

1.4 This PIA should be seen as an umbrella document for the Smart Metering Implementation Programme as a whole. The Government would expect that separate PIAs on individual practices are undertaken by all data controllers, such as suppliers, network operators and third parties, involved in the processing of smart meter data, prior to the mass roll-out of smart metering.

1.5 This document does not currently explicitly assess potential impacts in relation to non-domestic customers. Chapter 6 of the Government`s response to consultation contains further information on the approach to data access and privacy in the non-domestic sector[3].

Assessment Methodology – How were privacy impacts identified?

1.6 The Government has undertaken an internal assessment of potential privacy impacts associated with the smart metering programme. In the earlier stages of the Programme, the Privacy Security Advisory Group (PSAG) considered categories of data and compliance with privacy legislation. The Government has continued this process of stakeholder engagement

[1] Smart Metering Implementation Programme: Response to Prospectus Consultation - Supporting Document 1 of 5, Data Access and privacy, page 10 – 2.19-2.22
http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx#dcc

[2] Information Commissioners Office Privacy Impact Assessment Handbook version 2.0, Part 1: Background Information.
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

[3] DECC Smart Metering Implementation Programme Data access and privacy Government response to consultation (Nov 2012).
http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx#dcc

via the Consumer Advisory Group and the Data Access Group. The Government has also held workshops and bi-lateral meetings with a range of organisations, including suppliers, network operators, consumer groups, privacy groups, academics and third party organisations. These discussions have directly contributed to the identification of privacy impacts detailed in this document.

1.7 The Government has worked collaboratively with the Information Commissioner's Office throughout the development of the data access and privacy framework, and the Information Commissioner`s Office PIA Handbook[4] has provided guidance on the development of this PIA.

Assessment Methodology – What privacy impacts were identified?

1.8 The following potential privacy impacts were identified;

- Transparency: Consumer awareness of data collection and usage
- The use of half-hourly energy consumption data
- The management and release of data by the Data and Communications Company (DCC)
- Management of smart metering systems' security to protect against unlawful / unauthorised data access
- Use of data for other purposes by Government Departments, Local Authorities and Law Enforcement Agencies
- Third party access to more granular data
- Access to data after a change of tenancy
- Retention of smart metering data for longer than needed
- Access by non-account holders to energy consumption data.
- Deletion of data from the Smart Meter and In-home Display
- Visibility of data on the In-Home Display (IHD)

European Union Guidelines

1.9 The European Commission published a Recommendation on the roll-out of smart metering systems in March 2012. This included non-legally binding guidelines for member states on data privacy, including a recommendation that Data Protection Impact Assessments should

[4] ICO guidance on Privacy Impact Assessment is available at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

be carried out in all Member States to 'address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive 95/46/EC, taking into account the rights and legitimate interests of data subjects and persons concerned'[5]. In its Opinion of June 2012, the European Data Protection Supervisor also made recommendations about what should be covered in PIAs[6].

1.10 The European Commission is currently developing a voluntary Data Protection Impact Assessment template for Smart Grid and Smart Metering Systems. The template will be made available to organisations and member states. The Government will take account of any future developments at EU level, including the proposed PIA template, in future iterations of this PIA.

Privacy Enhancing Technologies (PETs)

1.11 The European Commission has issued a Communication supporting the development and use of privacy-enhancing technologies to minimise the processing of personal data and the use of anonymous or pseudonymous data wherever possible[7]. The Commission's Recommendation on preparations for the roll-out of smart metering systems also states that Member States should take all necessary measures to impose, as much as possible, use of data rendered anonymous in such a way that the individual is no longer identifiable[8].

1.12 Data controllers will need to comply with the Data Protection Act and other relevant legislation, and the Government response to consultation on data access and privacy sets out specific proposals on the levels of access that suppliers, network operators and third parties should have to energy consumption data, for which purposes, and the choices that consumers should have about this. The Government notes ongoing developments in the field of privacy-enhancing technologies, but feels that for smart metering it would be premature to mandate the use of any particular privacy-enhancing technology at this stage. However, consistent with the principles of Privacy by Design, and European Commission recommendations, the Government believes that parties wishing to access energy consumption data should wherever possible take steps to avoid or mitigate potential privacy concerns by:

- considering carefully whether data needs to be collected at all, and whether it needs to be collected from all customers; and
- aggregating or anonymising meter readings where it is not necessary to have personal data.

---

[5] Section 1.4. of 2012/148/EU: Commission Recommendation of 9th March 2012 on preparations for the roll-out of SM systems.
http://ec.europa.eu/energy/gas_electricity/smartgrids/smartgrids_en.htm

[6] Opinion of the European Data Protection Supervisor: EPS12/10 (June 2012)
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

[7] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) (May 2007)
http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

[8] European Commission Recommendation on preparations for the roll-out of smart metering systems (March 2012)
http://ec.europa.eu/energy/gas_electricity/smartgrids/smartgrids_en.htm

The Data Protection Act 1998

1.13 The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. The Government's policy on data access and privacy in respect of smart metering is designed to address more specific questions about the choices consumers should have about smart metering, and the levels of energy consumption data that it is appropriate for suppliers and others to access to carry out essential functions connected to the provision of energy. The Information Commissioner's Office has supported this approach, suggesting that sector-specific provisions, that complement the Data Protection Act, might be appropriate in the case of smart metering.

1.14 The Data Protection Act will continue to apply in conjunction with the smart metering regime that the Government puts in place. Suppliers and other data users will continue to have to comply with relevant requirements under the Act (for example, obligations to register with the Information Commissioner's Office and inform it about personal data being processed, and to comply with the eight data protection principles). Consumers will also retain their rights under the Act (including rights to access information held about them, to object to processing that is causing them distress, and to prevent processing for direct marketing).

Risk Review Process

1.15 The Government will follow the advice in the Information Commissioner's Office PIA handbook to ensure that further revisions of this PIA are undertaken as the Smart Metering Implementation Programme develops. As the roll-out of smart meters continues consumers will become more familiar with how smart metering data will be processed and used, therefore their attitudes and perceptions may change. In addition, the data access and privacy framework will evolve to take account of learning and best practice. The Government will ensure that subsequent Privacy Impact Assessments will take these factors into account when assessing any future risks.

Chapter 2 – Assessment of Risks

Potential privacy impacts, identified through the process of developing the data access and privacy policy framework, engaging stakeholders and consulting guidance from the Information Commissioner's Office, are set out below, along with measures for addressing those impacts, where appropriate.

Privacy Impact – Transparency: Consumer awareness of data collection and usage.

- **Smart metering will result in a step change in the granularity and frequency of energy consumption data that is available. Stakeholder groups have advised that some consumers believe that there are risks to their privacy relating to the processing of data and that such data could be used to identify their lifestyle and patterns of behaviour. There is a perception that data could be collected and used without the individual's knowledge, or that individuals could be targeted with unwanted information (for example direct marketing) based on their energy consumption data without their prior knowledge or permission.**

2.1 Recognising the concerns of some consumers, it is important that industry and third parties are clear with individuals concerning the processing of their personal data. This is why the Government has developed requirements within its data access and privacy framework to protect consumers.

2.2 The Government`s requirements have been developed to ensure a consistent approach to data protection and privacy, by specifying that parties using data provide appropriate information to their customers about this processing and by ensuring consistency in approach. Poorly presented information could lead to public opposition and negative media attention. Data controllers should ensure that consumers are provided with consistent and unambiguous information about their rights, as defined in the data access and privacy framework.

2.3 One of the principles of the data access and privacy policy framework is that individuals should have a choice about how their data is used, except where it is needed for "billing and Regulated Duties" for example, detecting and preventing theft. The Government`s framework contains measures to keep consumers informed about the choices they have made in relation to who is accessing their data and for what purpose. For example, the Government will require that suppliers and third parties should provide reminders to consumers about the data that they are accessing, and how consumers can change the arrangements if they wish to. In this way consumers can continue to control the choices they make.

2.4 In addition, in accordance with obligations under the Data Protection Act, data controllers must ensure consumers are notified via the use of fair processing notices and other terms and conditions notifications. This includes information about what data is being collected, the identity of the data controller and if the consumer has a choice as to whether the data can be

collected for that purpose. These notifications must be clear and unambiguous. Consumers should also be clearly notified before the processing of any such data takes place and any changes in these arrangements must be notified in good time[9].

2.5 In the Response to the Prospectus consultation (March 2011), the Government proposed that 'a privacy charter should be developed to provide clear reassurance to consumers as part of the overall consumer engagement package'[10]. The Government is looking to suppliers to develop the Charter, following finalisation of the framework for data access and privacy. Ahead of the development of the Charter, Energy UK have developed a set of voluntary Privacy Commitments[11], to help inform consumers about the steps their members will take to make sure that consumers are aware how and why their data is used, and the choices consumers have in sharing this data, prior to the finalisation of Government policy.

2.6 The Privacy Charter is not intended to take the place of regulatory requirements, but will need to reflect any regulatory framework that is put in place. Energy UK will continue to develop the Privacy Charter with the support of consumer groups and other industry representatives, and the intention is that this charter will be available when the data access and privacy framework comes into force.

Management Approach - summary

- In order to ensure consumers' interests are protected, the Government has developed a data access and privacy framework to provide clarity about the ways in which energy consumption data from smart meters can be accessed, by whom, for which purposes, and the choices that consumers should have about this. The requirements will be set out in supplier and network operator licences, and the Smart Energy Code

- An industry led Privacy Charter will be developed to provide clear reassurance to consumers about the ways in which their personal data will be used and the choices they have about this.

Privacy Impact - The use of half-hourly energy consumption data.

- **Arguments for and against allowing half-hourly data capture have been put forward by stakeholders, in working groups and in response to the Government's Call for Evidence and consultation on data access and privacy.**

2.7 The arguments around the use of half-hourly energy consumption data tend to vary between stakeholder groups. Some suppliers have argued that the processing of this data would lead to a greater realisation of benefits. On the other hand, consumer groups and

[9] Guidance on notification can be found at the ICO`s website: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_1.aspx

[10] Smart Metering Implementation Programme: Response to Prospectus Consultation, Supporting Document 1 of 5: Data Access and Privacy, pg 10, 2.23 & pg 11, 2.29 http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx#dcc

[11] Energy UK`s Privacy Commitments are available at: http://www.energy-retail.org.uk/smartmeters/smart-meter-policy-work

privacy advocates argue that privacy rights could be infringed from the processing of half-hourly data without consumer consent. More specifically, a concern is that data analysed at granular - level could indicate the daily habits and behavioural patterns of an individual or household, or lead to unwanted marketing activity.

2.8 Privacy and consumer stakeholders have also put forward the argument that where larger volumes of data are collected than are required for a particular purpose, it is possible that this capture of data could be excessive, and could result in a breach of the third Data Protection Principle (see Annex A).

2.9 As specified in Smart Metering Equipment Technical Specifications, the smart meter itself will be capable of storing up to half-hourly energy consumption data. More granular (near real-time) data will be displayed via the In-Home display and could also be collected and made available for the consumer to access using a Consumer Access Device that the consumer would have to obtain and connect securely to the Home Area Network. Only the consumer will be able to see this near real-time data, unless they have authorised another party to access that data.

Supplier access to data

2.10 The Government`s data access and privacy framework sets clear obligations about the granularity of energy consumption data that suppliers are able to access, for which purposes, and the level of choice that consumers should have about this. The basic framework, will:

- Allow suppliers to access monthly (or less granular) energy consumption data, for billing and for the purposes of fulfilling any existing statutory requirement or licence obligation;
- Allow suppliers to access daily (or less granular) energy consumption data for any purpose except marketing, with clear opportunity for the consumer to opt out; and
- Require that suppliers must receive explicit (opt-in) consent from the customer in order to access half-hourly energy consumption data, or to use energy consumption data for marketing purposes.

2.11 In addition, obligations under the Data Protection Act specify that in order to mitigate the risk of excessive or unnecessary data processing, "personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed"[12].

Network operator access to data

2.12 The Government`s framework also specifies that before they have access to granular data for Regulated Duty purposes, network operators will need to develop and submit for approval plans detailing how privacy concerns would be addressed (for example through aggregation) and what the data would be used for. Aggregation, where appropriate, can help to address any privacy concerns in the sense that information about individuals

[12] Data Protection Act 1998, Schedule 1, Part 1(3)

cannot be identified from the data. There are outstanding questions around how aggregation will work in practice (it is assumed that individual data would still need to be collected from source, and at least one entity would have access to this disaggregated data, at least for a short period of time, although in future privacy enhancing technologies may obviate the need for this).

Third Party access to data

2.13 In terms of third parties, the granularity of data used will depend on the terms and conditions of the service that consumers consent to. Where consumers give third parties permission to access their energy consumption data remotely via the DCC, third parties will have to comply with arrangements to protect consumers, in the Smart Energy Code.

2.14 Capability for smart meters and IHDs to display a Customer Identification Number has been built into SMETS, and data and communications services are being procured on the basis that the DCC will need to be able to send these CINs as a means to verify individuals within the premises. However, the Government has not yet decided on precisely how this should work in practise, such as whether the CIN approach should be purely optional, as one way for third parties to verify the individual, or whether it should be mandatory.

Management Approach - summary

- The Government`s framework specifies the conditions, including level of granularity, under which data can be obtained by licensees and others for different purposes. The Government has set out these requirements in the form of obligations within licence conditions or the Smart Energy Code, as appropriate.

- The data access and privacy framework also specifies that network operators will need to submit plans on how they would use aggregation or other privacy enhancing methods before accessing detailed data.

- Current obligations that exist for all data controllers in the Data Protection Act and Privacy and Electronic Communications (EC Directive) Regulations will also apply.

Privacy Impact – The management and release of data by the Data and Communications Company (DCC).

- **The Data and Communication Company (DCC) will be the conduit for most domestic and some non-domestic consumers' data as it travels from their smart meter to those parties which are authorised to have access to it. The DCC and its data and communication service providers will have to meet requirements on transmitting data. Given the volume and detail of the data it is important that data is transmitted securely and processes are put in place to ensure that data remains secure and privacy is protected.**

The DCC`s role in relation to data access

2.15 Once it is established, the DCC will manage system data relating to the functioning of the meter, data and communication systems, but will not act autonomously in determining whether to collect data relating to the consumption of energy by consumers. For consumption data, the DCC will only respond to instructions from authorised users (such as suppliers, network operators and third parties) to:

a) retrieve consumer data stored on the meter on behalf of the data controller or an authorised requestor e.g. retrieve a meter 'reading';
b) send data or instructions to the meter e.g. in regard to setting a new tariff; or
c) convey an alert message from the meter to an authorised data controller.

2.16 Where the DCC is transmitting data on instruction from the authorised data controller, it would be the responsibility of the data controller to manage their own obligations under licence conditions, the Smart Energy Code and the Data Protection Act and any other relevant legislation, as appropriate. If they do not, relevant sanctions would apply to that data controller.

2.17 The Government intends to make clear through the Smart Energy Code that the DCC will fulfil its role in line with the Data Protection Act, and in a way which does not prevent others from fulfilling their own obligations[13]. There will also be high-level obligations on the DCC to protect the physical integrity of the smart metering system and transmit confidential information appropriately. The obligations on the DCC are set out in the Government Response to the consultation on the draft DCC Licence Application Regulations and the Government Response to the consultation on the draft DCC Licence[14].

2.18 The DCC will only transmit consumption data once it has received a data request from an authorised requestor. It will not collect consumer data of its own volition or in anticipation of an authorised request. The DCC will perform checks to determine whether a data request has originated from an authorised requestor. These checks include whether the requestor is a signatory of the Smart Energy Code, and where appropriate, the registered supplier for the meter point in question. As described above, the DCC will only act on instruction from an authorised data controller and so cannot determine whether a data request is proper or not. In requesting data from the DCC, requestors would effectively be confirming (or self-certifying) to the DCC that they had the necessary permission to access the data, where this was required.

2.19 Given that the DCC will not originate requests for consumption data, the DCC is not expected to store consumption data except in short term buffering periods, which it would use to manage its flow of data requests and system data messages effectively. It will also not be under any obligation to inform data subjects that it is transmitting data. It will be the responsibility of the requesting data controller to inform data subjects what data is being

[13] Smart Metering Implementation Programme: Stage 1 of the Smart Energy Code – a Government response and a consultation on draft legal text (November 2012)
http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx
[14] Smart Metering Implementation Programme: Government response to the consultation on the draft DCC Licence Application Regulations (Sept 2012) and Government Response to the consultation on the draft DCC Licence. (November 2012)
http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx

transmitted. The Government responses to the consultations on the draft DCC Licence Application Regulations and the draft DCC Licence[15] set the proposals for the role of the DCC and the scope of its activities.

2.20 The Government is continuing to consider the arrangements for ensuring that third parties (and suppliers where they are not the registered supplier) verify that any request for data access comes from the individual in the premises in question.

Management Approach - summary

- The DCC Licence Conditions (Provision 10) include a General Prohibition not to release 'confidential data', which includes energy consumption data, without authorisation.
- DCC authorised users will be required to comply with their obligations under the Data Protection Act and be required by licence (or the Smart Energy Code) only to access data in accordance with appropriate consumer choice mechanisms, with defined sanctions where non compliance is identified.
- The DCC will be required to adhere to its obligations, and process data according to the Data Protection Act.
- The DCC will perform access control checks before data is released to ensure that the requestor is an authorised party.

Privacy Impact – Management of smart metering systems' security to protect against unlawful / unauthorised data access.

- **Stakeholder groups have highlighted the need to ensure that personal data contained within the smart metering system, including the meter itself, the communications hub, the Home Area Network (HAN) and the Wide Area Network (WAN), could be compromised through a breach in security allowing unlawful / unauthorised access.**

2.21 In order to ensure the ongoing security of smart meter systems the Government is taking a 'security by design' approach, in which security concerns are considered and addressed at every stage throughout the development lifecycle. To support this approach, the Government has produced security requirements to mitigate the anticipated risks that the end-to-end smart metering system will introduce.

2.22 These requirements can be found in a number of the Government's publications including; the Smart Metering Equipment Technical Specifications (SMETS 1 & 2), the Government

[15] Smart Metering Implementation Programme: Government response to the consultation on the draft DCC Licence Application Regulations (Sept 2012) and Government response to the consultation on draft DCC Licence. (November 2012)
http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx

response to the consultation on the draft DCC Licence Applications Regulations and the Government response to a consultation on a licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters[16].

2.23 The Smart Metering Equipment Technical Specifications (SMETS 1 & 2) will provide a sound basis for suppliers installing compliant meters to be able to operate them securely. The security requirements provide for key security controls in areas such as the encryption of sensitive data, checks on the validity of critical commands sent within the system, and the tamper resistance of metering equipment (amongst other areas).

2.24 The Government`s Consultation on the second version of the Smart Metering Equipment Technical Specifications considered how security requirements should be governed, and the regimes that will be required to provide appropriate levels of assurance in respect of both security and interoperability[17]. It also proposed a similar regime for those compliant meters not enrolled with the DCC.

2.25 The Government has been working closely with relevant agencies and experts in developing policies and arrangements. The Government has developed its policy proposals in a properly structured and rigorous way, in collaboration with relevant Government agencies and other experts such as CESG, to identify challenges in order to ensure an appropriate level of security within the smart metering system.

2.26 In addition, the Government is developing an assurance regime that will enable security arrangements to be reviewed on an ongoing basis in order to maintain the security of smart metering systems.

2.27 In October 2012, the Government published a response to its consultation on the draft licence condition with regard to obliging suppliers to carry out security risk assessments and independent annual audits for their smart meter end to end systems in the period before the Data and Communications Company starts to deliver services.

The DCC and mandating certain security requirements / standards of security.

2.28 Before the DCC starts to provide services, suppliers as data controllers are responsible for the security of their end-to-end smart metering systems. Data controllers are able to work with their service providers to consider how to operate their systems in a secure way which is most appropriate to the technology they use. For the period after the DCC starts to provide services, the Smart Energy Code will set out the requirements and governance arrangements for security on an ongoing basis.

Management Approach - summary

[16] The DECC, Smart Metering Implementation Programme: Government response to a consultation on a licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters (Nov 2012). http://www.decc.gov.uk/en/content/cms/consultations/smart_mtr_sec/smart_mtr_sec.aspx

[17] Smart Metering Implementation Programme: Consultation on the second version of the Smart Metering Equipment Technical Specifications: August 2012, Section 5 http://www.decc.gov.uk/en/content/cms/consultations/smets2cons/smets2cons.aspx

- The Government has developed security requirements to minimise: (i) the likelihood of a successful attack on smart metering infrastructure, and (ii) the impact should it occur.

- The Government will develop an assurance regime that will enable security arrangements to be reviewed on an ongoing basis to ensure the security of smart metering systems.

- The Government has published its response to a consultation to a licence condition with regard to obliging suppliers to carry out security risk assessments and independent annual audits for their smart meter end to end systems in the period before the Data and Communications Company provides services to smart meters[18].

- The Government is continuing to develop procedures which the DCC will implement in order to ensure the security of the systems which it will operate when it comes on-line in late 2014.

Privacy Impact – Use of data for other purposes by Government Departments, Local Authorities and Law Enforcement Agencies.

- **Some stakeholders have raised questions about the potential use of smart metering energy consumption data by law enforcement agencies, local authorities and central Government departments, and about the extent to which this would impact on consumers' privacy.**

2.29 Smart meter data potentially offers more detailed information about energy usage than had previously been available, and this may lead to increased requests for access to personal data from law enforcement agencies (such as the police). Data controllers should ensure they have procedures in place to deal with requests for access to energy consumption data and ensure appropriate safeguards are established before disclosure of data. Data controllers should take care to verify that the request is from an appropriate authority and be satisfied that the authority has stated that the disclosure of the data is necessary for the purposes of crime prevention or detection, or the apprehension or prosecution of offenders in line with existing legislation.

2.30 The processing of personal data by appropriate authorities is permitted under Schedule 2 (5) of the Data Protection Act, if it is deemed to be necessary for administering justice, or for exercising statutory, governmental, or other public functions exercised by any Government department if it is in the public interest. It is important to note that data that is produced by conventional meters is currently legitimately accessed by public bodies.

2.31 The Government will need to have access to some smart metering data for the purposes of statistical analysis, monitoring and evaluation of the Smart Metering Implementation Programme. This will include analysis of periodic (e.g. quarterly) energy consumption data

[18] The DECC, Smart Metering Implementation Programme: Government response to a consultation on a licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters (Nov 2012) http://www.decc.gov.uk/en/content/cms/consultations/smart_mtr_sec/smart_mtr_sec.aspx

at meter level to measure changes in annual consumption due to the impact of smart meters for at least a sample of customers. Analysis will be reported at aggregate level (for example, industry and socio-demographic level). The entire data life-cycle from data source inputs through to reporting results will operate within the bounds of the Data Protection Act, but also more generally, following recommendations set out in the Government`s Data Handling Procedures Report 2008 and the Code of Practice for Official Statistics 2009.

2.32 The Government has set out its approach to requesting information from suppliers and network companies in the Response to the consultation on information requirements for monitoring and evaluating the roll-out of smart meters[19]. The document specifies the general approach to meeting the Government`s information needs, and sets out the regulatory framework within which the Government will specify in detail the content, format and timing of information requests to energy suppliers and network companies. The document sets out the level of granularity at which the Government is minded to request data. The intended approach to publication of data is also discussed, reflecting the requirements of the Data Protection Act 1998 and the restrictions on disclosure set out in section 105 of the Utilities Act 2000**.** The use of smart metering data will also be considered in the context of the Government's broader transparency and Open Data agenda[20].

2.33 DECC intends to carry out a separate Privacy Impact Assessment in respect of the data it uses for monitoring and evaluation purposes.

Management Approach

- The Government`s Strategy and Consultation on information requirements for monitoring and evaluation gives further consideration of the instances in which the Government may wish to access data, and the means by which it will be provided with access.

Privacy Impact - Third party access to more granular data

- **Discussions with stakeholders have highlighted a need to ensure that where they are sending more granular (i.e. half-hourly or more detailed) data on to third parties in order to receive a specific service, consumers are clear about the implications of doing so.**

2.34 The Government is clear that consumers should be able to access their own smart metering energy consumption data easily, and share this with third parties, should they choose to do so. In the first version of its Smart Metering Equipment Technical Specifications document, the Government specified a minimum requirement that daily data would be visible on the In-Home Display. However, consumers will be able to capture their

[19] Smart Metering Implementation Programme: Government response to the Consultation on information requirements for monitoring and evaluation: http://www.decc.gov.uk/en/content/cms/consultations/sm_evaluation/sm_evaluation.aspx

[18] More information on the Open Data initiative is available at; http://www.cabinetoffice.gov.uk/news/making-open-data-real-consultation-summary-responses

more detailed energy consumption data – at a frequency dependent on the Home Area Network technology used in the metering equipment, but required to be better than ten seconds - by connecting an additional 'Consumer Access Device' to the Home Area Network. This more granular data would then be visible via the Consumer Access Device, which could be a piece of equipment that connects to an existing WiFi router. The process for connecting a third party device will be consumer friendly and secure, to prevent someone else from accessing an individual's data by connecting a device to their Home Area Network. The Consultation on the second version of the Smart Metering Equipment Technical Specifications includes proposals on how this process could work[21].

2.35 Consumers could choose to send this data onto third parties if they wished to. As with any competitive market, such arrangements would be governed by contract between the consumer and third party - for example, an individual would agree to terms and conditions when signing up for a particular service - and would be outside the scope of the smart metering regulatory regime. Third parties would be bound by relevant legislation such as the Data Protection Act. The Government does not consider it necessary or appropriate to introduce any specific measures in respect of these transactions, other than the requirement within the Smart Energy Code that all third party entities accessing data via the DCC must provide their customers with reminders about the data that they are accessing, and how consumers can change the arrangements if they wish to[22]. In this way the consumer can continue to control the choices they make.

2.36 However, the Government is conscious that data captured via the HAN which is sent on to third parties could include more granular near real-time data, which could allow appliance-level use to be identified and which prompts the greatest privacy concerns. Whilst consumers would explicitly have to agree to the collection of this information (for example, they would need to acquire an additional device to enable this), it is important that consumers are clear about what is involved. The Government is therefore discussing this issue with manufacturers of relevant devices to encourage good practice.

Management Approach - summary

- The Smart Energy Code will include requirements to protect consumers interests with regard to transactions with third parties.
- Data controllers will be responsible for providing clear information to consumers about the uses to which data will be put, and the choices that consumers have about this.

Privacy Impact - Access to data after a change of tenancy.

[21] Smart Metering Implementation Programme – Consultation on the second version of the Smart Metering Equipment Technical Specifications:
http://www.decc.gov.uk/en/content/cms/consultations/smets2cons/smets2cons.aspx

[22] Smart Metering Implementation Programme: Stage 1 of the Smart Energy Code – a Government response and a consultation on draft legal text (November 2012)
http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx

- **Stakeholders from the energy industry and consumer and privacy groups have indicated that there is a risk that a new tenant may try to access the previous tenant's energy consumption data, either via the DCC or over the Home Area Network (HAN) directly.**

2.37 As the smart metering system will retain up to 13 months of consumption data within the meter, incoming residents may try to access the historic consumption data of the previous resident either in error or deliberately.

2.38 The Government has included a security capability in the Smart Metering Equipment Technical Specifications (SMETS) to restrict access to data. This capability will be activated once the outgoing tenant informs their supplier that they will be moving home. The supplier will then send a request to apply a 'restrict data command' to the relevant data items (e.g. 13 month profile data) stored in the smart metering equipment. No party will be able to access historic energy consumption data from the meter itself or remotely up to and including the date set by the command[23]. The responsibility is on the consumer to notify the supplier of a change of tenancy, in order for the 'restrict access to data command' to be applied to that consumer's meter. As data relating to the period up to and including the date specified by the command cannot be accessed, data controllers should ensure that data that they may require is accurate and kept up to date in accordance with their obligations under the Data Protection Act.

2.39 Where a consumer is on a prepayment plan with their supplier and their meter is hard to access, they may be issued with a Prepayment Interface Device. This Interface Device would ordinarily be owned by the supplier and as with the IHD, any data relating to the previous tenant would need to be erased on change of tenancy.

Management Approach - summary

- The SMETS Electricity and Gas Meter documents detail the security capability to restrict access to data that will protect against unauthorised access of data.

Privacy Impact - Retention of smart metering data for longer than needed.

- **Data controllers need to be able to collect data for a number of purposes, but there is a perception and potential privacy impact that data controllers could hold on to it for longer than they need to.**

2.40 The collection and retention of data by data controllers will need to satisfy obligations under the Data Protection Act.

[23] It may be possible that the supplier or network operator might have their own historical data in regard to the previous tenant, if they are the same supplier / network operator for the new tenant. However, that same supplier/ network operator, as the data controller, should ensure that they are only accessing that data in line with licence conditions and obligations under the Data Protection Act.

2.41 The Government will rely on the fifth Data Protection Act Principle in regard to the timescale for which data should be retained by data controllers or data processors. This principle is that personal data processed for any purpose, or purposes, shall not be kept for longer than is necessary for that purpose or those purposes.

Management Approach – summary

- The Government recommends that data controllers should consider how consumers are notified about data retention policies and that data retention should be in line with their obligations under the Data Protection Act. Data controllers should also review their policy on data retention and consider the purposes to which data is put.

Privacy Impact – Access by non-account holders to energy consumption data.

- **Where a customer holds an account with a supplier, that customer may be concerned that a non-account holder may gain access to their energy consumption data without the customer`s permission. The customer`s data might then be used where that customer is not fully aware of such usage.**

2.42 Suppliers have their own internal policies and procedures in relation to this privacy impact. Suppliers have confirmed that only account holders will be able to gain access to the customer`s account and the details contained on that account (including that customer's energy consumption data). Any non-account holder that wishes to see this data must submit to the processes that the supplier has prescribed in order to become a named account holder. These processes ordinarily entail that the account holder is made aware of this process and must approve it.

2.43 Third parties would be bound by relevant legislation such as the Data Protection Act. The Government does not consider it necessary or appropriate to introduce any specific measures in respect of these transactions as these procedures have been in place and have operated effectively for some time.

Management Approach – summary

- The Government recommends that data controllers should consider how consumers are notified about any applications made by non-account holders. Data controllers should also review their policy periodically to ensure that it is still fit for purpose.

Privacy Impact – Deletion of data from the Smart Meter and In-Home Display.

- **Stakeholders from the energy industry and consumer and privacy groups have indicated that consumers may be concerned that their energy consumption data is not deleted from the Smart Metering System and could be accessed either via the DCC or over the Home Area Network (HAN).**

2.44 The Government`s first version of the Smart Metering Equipment Technical Specifications (SMETS 1) requires that the electricity and gas smart metering system stores up to 13 months` consumption data. There is no requirement to enable the deletion of data, but there is a requirement for the metering equipment to have a secure perimeter (physical and communication) to prevent unauthorised access to data. In addition there is a requirement for 'restrict access to data flags' in the data store to prevent access to data that has been generated, for example, by a previous tenant. The responsibility is on the consumer to notify the supplier in order for the 'restrict access to data flag' to be placed onto that consumer's meter. Suppliers have a licence obligation to ensure that installed equipment is SMETS compliant.

2.45 Once the DCC is operational it will also apply 'restrict access to data' flags. This capability will be activated for example once the outgoing tenant informs their supplier that they will be moving home. No party will be able to access historic energy consumption data from the meter itself or via the DCC up to and including the date set by the flag.

2.46 The minimum specification In-Home Display (offered to consumers by suppliers as part of their roll-out obligation) has no requirement to store data, and as such there is no requirement for deletion of data / restricting access to data. In addition, the minimum specification In-Home Display (offered to consumers by suppliers as part of their roll out obligation) is owned by the consumer. The consumer is therefore responsible for controlling access to any data that is displayed on it. Where a supplier has given a consumer a display that exceeds the minimum requirement (e.g. a display that has the ability to store data) and it is owned by the consumer, the consumer will be responsible for protecting the data stored on it.

Management Approach – summary

- The Government`s first version of the Smart Metering Equipment Technical Specifications requires that all equipment components must be physically and communications secure. The responsibility will sit with the supplier and meter manufacturers to meet these requirements, up to the period the DCC becomes operational and once it is operational.

- The SMETS Electricity and Gas Meter documents detail the 'restrict access to data flag' that will protect against unauthorised access of data by any party that wishes to access data relating to the individual's energy consumption, who does not have the appropriate authorisation, and / or prior to that individual becoming their customer or any subsequent inhabitant of the property to which the data relates.

Privacy Impact – Visibility of data on the In-Home Display (IHD)

- **Most consumers will choose to place their In-Home Displays (IHDs) in open view within their premises. There is a risk that a consumer's energy consumption data and other information, such as financial data, will be visible to visitors.**

2.47 In-Home Displays will ordinarily be located inside a consumer's premises, and under the control of the consumer, who will be able to decide whether or not others visiting their premises should be allowed to see the IHD.

Management Approach - summary

- Consumers will have control of the location and visibility of the IHD and will decide who can see the data

Chapter 3 – Next Steps

3.1 This Privacy Impact Assessment should be read alongside the Government`s Response to the consultation on smart metering data access and privacy[24].

3.2 The Government will continue to adopt a Privacy by Design approach to the delivery of smart metering. There will be a need to review this PIA in light of policy decisions that are made and risk-mitigating actions that are taken during the next phase of the programme.

3.3 We will look to review and update this document if there are further developments, including at EU level, and in light of ongoing discussions with stakeholders regarding data access and privacy issues.

[24] http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx#data

Annex A – Data Protection Principles

Schedule 1 of the Data Protection Act 1998 (DPA) lists the Data Protection principles as the following:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

    a. at least one of the conditions for processing, listed in Schedule 2 of the DPA, is met and

    b. in the case of sensitive personal data, at least one of the conditions listed in Schedule 3 of the DPA is met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any matter incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Annex B – Key Assumptions

Definitions

Personal data are defined in the Data Protection Act[25] as "…data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller". The Government's view is that energy consumption data from domestic smart meters should be considered to be personal data for the purposes of the Act[26]. This view is supported by the Information Commissioner's Office and Opinion 12/2011 of the Article 29 European Data Protection Working Party[27].

There are arguably some circumstances in which energy consumption data from a smart meter might not constitute personal data – for example where it relates to more than one individual in a household, but the Government believes it appropriate to adopt a precautionary, protective approach and assume that energy consumption data is personal data. A range of parties may wish to access other types of smart metering data, such as technical data required by network operators. In some cases such data may still constitute personal data according to the Data Protection Act, and in these cases, obligations under the Data Protection Act would apply.

Data Subject: The Data Protection Act defines the data subject as "the individual who is the subject of the personal data"

Data Controller: Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. The Act defines a data controller as "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed". It is the legal responsibility of all industry participants to ensure that they comply with the Data Protection Act (and any other relevant legislation) to the extent that it applies to them. Under the Data Protection Act, data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Generally speaking, suppliers, network operators and third parties accessing energy consumption data are likely to be data controllers.

Data Processor: The Act defines data processor as "in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller". The Data and Communications Company (DCC) will be potentially acting as a data processor on behalf of data controllers, although this will depend on the exact nature of the activity being undertaken and the contractual basis for it.

[25] Data Protection Act 1998, Part 1, Section 1(1)(e)
[26] Other data, that is not energy consumption data, may also be considered personal, if it can identify an individual from that data, such as financial data.
[27] Article 29 Data Protection Working Party Opinion 12/2011 on smart metering. Adopted 4 April 2011: 00671/11/EN wp183:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Department of Energy & Climate Change
3 Whitehall Place
London SW1A 2AW
www.decc.gov.uk

URN 12D/023