SUMMARY POLICY ISSUE PAPER

Title of Paper	**Privacy Impact Assessment & Information Risk Assessment**		
Issue Ref		Date: 5 July 2016	
Issue Owner	Jenny Boothe		
Author	Niko Kalfigkopoulos		
Discussed at User Group	11 July 2013		
Issued to DA			

Summary

1. In early 2015 the Office of Gas and Electricity Markets (Ofgem) published a decision to introduce reliable and fast switching for consumers between gas and electricity suppliers using a Centralised Registration Service (CRS) (the Switching Programme).

2. PwC was engaged to conduct a Privacy Impact Assessment (PIA) and an Information Risk Assessment (IRA) of the design of the Switching Programme, in order to identify key data privacy and information concerns and provide an explanation of their associated risks. The output of these two exercises is contained within the PIA and IRA reports.

3. Both the PIA and IRA activities were conducted in the blueprint phase prior to final decision on the data to be captured/orchestrated by the CRS and prior to the decision on the solution architecture.

Analysis

4. The PIA report sets out the following analysis:
   - It identifies and describes key concepts and principles under the General Data Protection Regulation (GDPR) that are relevant to the identified architecture design solution models for the CRS under the Switching Programme (the Strategic Themes).
   - Based on the outcome of the GDPR analysis, the PIA Report includes an analysis of the key data protection and data privacy risks relevant to the Strategic Themes.

5. Why is a PIA necessary:
   - It is anticipated that the CRS will handle a high volume of data - some of which may be classified as sensitive personal data - and as such it is crucial to take into account data protection and data privacy considerations.

- Whilst conducting a PIA is currently regarded by the Information Commissioner's Office as being best practice, the General Data Protection Regulation (GDPR) makes PIAs and "Privacy by Design" an explicit requirement during the design phase of a new processing purpose or system.
- Conducting a PIA at this early stage identifies and raises the awareness of the applicable data-related requirements that the Switching Programme solutions will be subject to under the GDPR.

6. The IRA report sets out the following analysis:
   - It identifies the various Threats that may accidentally or with malicious intent impact the Switching Service, resulting in the breach of Confidentiality, Integrity or Availability of information and systems.
   - It outlines the various techniques that a Threat might use to disrupt the service.
   - It indicates at a high level the various controls necessary to be designed and implemented in the solution, to reduce the inherent risks identified in this report.

7. Why is an IRA necessary:

Information is the heart of the Switching Programme. The principles of Confidentiality, integrity and availability of information are key for reliable and secure switching. The IRA helps to:

- Take a risk-based informed decision for the design options, considering all the aspects of people process and technology
- Identify the key information risks at early stages to influence the design before this is formalised
- Consider the mitigation controls (both technical and administrative) for the risks that will be applicable to the switching service
- Consider the influence of various stakeholders and their level of access to the CRS, as a key risk for the switching programme
- Raise awareness amongst the various stakeholders of the switching programme to plan and accommodate for changes in the current governance model, and the factors they need to consider to manage information risk.

Key Findings (PIA)

The details of the key findings are set out in the Annex to this paper.

There are fundamental decisions to be made as to the data relationships between the parties involved in the Switching Programme.

- No decision has been made regarding which entity would be the Data Controller.
- No decision has been made regarding which entity would be the Data Processor, or whether there are multiple Data Controllers and one or more Data Processors.
- No decision has been made regarding whether any sub-processors would be required.

8. The CRS will involve the processing of customers' personal data, and possibly processing sensitive personal data.

9. Where personal data is being processed, data protection legislation requires that at least one of the entities involved in that processing takes ownership and responsibility for ensuring compliance with the applicable legal requirements, as a "Data Controller".

10. In the present stage of the design of the Switching Programme, it is not clear which of the entities involved will take that role.

11. The Strategic Themes present a number of options in this regard. For example, it may be appropriate for the CRS agent to take up the role of "Data Controller" and assume responsibility for the data processed. Alternatively, it may decide that it is more appropriate to assume the role of "Data Processor", and take instructions from the other entities involved.

12. This PIA Report sets out some of the key implications attached to these options, to aid this decision making process.

There are key operational privacy issues that need to be addressed as part of the next phases of the programme.

- Ensuring and maintaining data accuracy has not been addressed.
- The type of, and responsibility for, policies and procedures has not been addressed.
- Governance arrangements have not been addressed.

13. Operational privacy encompasses requirements for data quality (for example, that information should be accurate), data retention and data security, requirements concerning the purposes for which data can be handled and shared, requirements for transparency about handling.

14. Because the Switching Programme is still at design stage, a data governance framework has not yet been formulated, nor are there internal policies and procedures to ensure that operational privacy requirements are met.

15. This PIA report sets out the application of some of these core elements of operational privacy, as required by the GDPR, and their application to the Strategic Themes.

There are key legal privacy issues that need to be addressed.

- No decision has been made regarding what data sets will be included in the CRS.
- No decision has been made regarding the lawful basis under which data would be processed.
- No decision has been made regarding defining the purpose for which data is processed under the Switching Programme.

16. Again, because the Switching Programme is still at design stage, some key legal privacy requirements have not been addressed, such as how the Switching Programme addresses the data minimisation[1] and purpose limitation[2] principles.

17. This PIA Report sets out the application of some of these core elements of legal privacy, as required by the GDPR, and their application to the Strategic Themes.

Next steps

A further PIA and IRA will be required once the final architecture is agreed.

18. The current PIA and IRA reports are at a necessarily high level, because they were conducted during the blueprint phase of the Switching Programme and some of the fundamental aspects of the Switching Programme have not yet been formed. Once a final architecture solution has been agreed for the CRS, and once the fundamental issues set out at the key findings above have been addressed, it will be necessary to conduct further iterations of the PIA and IRA to identify the data privacy and information risks associated with the final solution and to make recommendations to mitigate against residual risks.

'Privacy by design' and 'security by design' principles should be adopted.

19. The programme should factor in the findings from the PIA and IRA reports, and incorporate security and privacy requirements that may be necessary in the design solution blueprint. These requirements should form part of the decision making process, as well as the detailed requirements list for building the solution in the future.

A risk governance and management framework should be established.

20. The programme should establish a framework that will allow the ongoing management, treatment and monitoring of security or privacy risks to the switching service. These should include findings/issues from both the PIA and IRA exercises.

Update from User Group

21. The User Group (11 july) noted the summary paper. They felt that it was good that the PIA/IRA was undertaken at this stage of the programme and understand that there will be further iterations of both documents as the programme progresses. No further comments were received.

[1] The GDPR specifies that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). This principle guards against processing excessive, superfluous amounts of data.

[2] The GDPR, in Article 5, specifies that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Annex 1

Key Findings (IRA)

1.	**The main strategic themes have inherent information risks, which should be acknowledged in the decision making process by the programme.**	A fundamental business decision has to be made regarding the solution architecture, considering the risks posed by each theme. Both the solution themes have inherent risks which should be considered. Theme 1 • There is a single point of failure for the CRS system, increasing the importance of system reliability, availability and resilience. • The centralised database will support third party organisations (e.g. MIS), hence, the risks pertaining to other systems may also impact the CRS system. • A single source (CRS) holding all customer data is a target likely to attract multiple threats aiming to disrupt or compromise the service. • Due to the reliance of data originating from multiple external sources, there is a risk to the accuracy and integrity of the data reconciliation. • The complexity and potential issues stemming for the data reconciliation process may introduce delay to the programme's timelines. Theme 2: • The CRS system will have a dependency on external stakeholders' ability to

		maintain information security and resilience of the systems supported by multiple technologies. This poses a key risk to the programme, which it cannot address or manage directly. • The accuracy of customer data collected from multiple sources may vary, both in terms of accuracy as well as timeliness. This can potentially affect the 'Next Day' switching target timelines. • The custom software for the middleware solution risks creating new vulnerabilities in the systems, due to the inherent lack of long-term operational testing. This may increase the risks of the switching service being compromised by external attacks.
2.	**The switching service is dependent on multiple external stakeholders for the effective operations and resilience of the service.**	The success of the switching service heavily relies on the effective and secure operation of the various external stakeholders involved. In order for DCC to gain assurance over third party security, the following should be considered: • DCC requesting external stakeholders to conduct information risk assessments periodically, notifying the DCC of any critical issues that may impact the switching service. • DCC obtaining Smart Energy Code compliance reports from external stakeholders to ensure they are effectively managing security and not introducing additional risks to the switching service. • DCC requesting the right to audit stakeholders periodically, to ensure their operational security effectiveness. Risk context: 1) An existing supplier who is losing business may disrupt or delay the process by compromising the integrity of customer data, resulting in the delay of the switching process. 2) Errors made by an authorised user when operating information systems as a result of carelessness, negligence or omission (e.g. insufficient care in processing information, or

		intentionally disregarding organisational policies, standards and procedures).
3.	**The compromise of the CRS system may have an impact to the operation of Smart Metering in GB.**	Smart metering functionality will rely on data being appropriately managed and processed by the switching programme. An incident occurring in the switching service leading to a compromise of confidentiality, integrity or availability of the CRS system is likely to impact smart metering operations in GB. Considerations to manage the impact of this risk may include: • Identified the key data points or data sets that are critical for operations of both the switching and smart metering programmes • Providing adequate security controls to ensure the protection of the identified key data points • Enforcing strict access controls on the systems identified as having the potential for a 'knock on effect' to smart metering Risk context: 1) A user account with access to both the CRS and smart metering systems could be compromised (e.g. using the Phishing technique) and used to gain access critical systems. 2) A stakeholder modifying key data sets (intentionally or accidentally) in the CRS may have a detrimental effect to smart meter operations.
4.	**There are currently no information security standards or risk governance frameworks established for the switching service.**	A security baseline is fundamental to support the ongoing security assurance of the switching service, as it will establish a common framework that all future information assurance activities will be based on and assessed against. This can be achieved by: • Adopting industry recognised standards for security baseline such as ISO 27001, ISF Standard of Good Practice, NIST. • Establishing a risk management governance framework for ongoing information risk assessments such as ISO

		27005, IRAM2. Risk context: Without a security baseline and framework in place, the implementation of the switching solution would risk having unidentified gaps that may result in the delay to the programme's milestones/deadlines.
5.	**The switching service (especially Theme 1) is likely to be a high-value target of sophisticated and advanced threats.**	The design of the solution architecture should consider: • Multi-layer protection (Defence in depth) • Security operations monitoring • Built-in resilience against vulnerability attacks and advanced persistent threats • Ongoing assurance through penetration testing and vulnerability assessments. Risk context: The CRS system is likely to hold critical and sensitive data related to switching as well as smart metering operations, making it a highly attractive target; sophisticated threats are likely to build custom-developed malware to target the CRS system or the users of the system using advanced attacks.
6.	**New stakeholders who gain access to the CRS may pose additional information risks to the Switching Service.**	The new business processes supporting the switching service may require new stakeholders obtaining access to the CRS data (e.g. TPI getting access to objection data). As such, there should be a formal decision process on allowing access to third party entities, which takes under consideration: • A risk-based approach to grant authorisation for access. • New stakeholders should comply with DCC's information security requirements. • Access to the data used and processed for the agreed intended purpose (as per GDPR requirements). Risk context: A TPI having access to customer personal information including 'Objection' data may use that data for targeted advertisement. This would violate GDPR requirements.

7.	**A supplementary IRA will be required to identify the residual risks of the designed solution.**	Once the solution design is formalised, an additional IRA will be required to ensure: • The risks identified in the current iteration are addressed by the design principles of the solution design. • The effectiveness of the planned controls in mitigating identified (or future) risks. • Plans and processes are in place to address the residual risks through risk treatment options. It is also advisable to consider carrying out a further risk assessment once the switching service is in 'live' operation. This is to determine the operational effectiveness of the designed controls, to monitor ongoing risks and to provide assurance of the secure operation of the switching service. Risk context: The current assessment identifies the programme's inherent risks for consideration as part of the selection of the final design. An assessment at a later stage will identify the exact mechanisms and gaps to address the residual risks of the switching service.