Representation - Draft Modification Report 0593V

Provision of access to Domestic Consumer data for Price Comparison Websites and Third Party Intermediaries

Responses invited by: 5pm on 08 September 2017

To: enquiries@gasgovernance.co.uk

Representative:	Andrew Margan
Organisation:	Centrica Plc
Date of Representation:	06 September 2017
Support or oppose implementation?	Qualified Support
Relevant Objective:	**d)** Positive

Reason for support/opposition: Please summarise (in one paragraph) the key reason(s)

The CMA Energy Market Investigation (ECOES/DES) Order 2016 seeks to remedy weak domestic customer switching responses. Modification 0593V seeks to permit Transporters (and their Agency) to make available industry data, to Price Comparison Websites (PCWs), through access to centrally held industry data items. The Agency, now the Central Data Service Provider (CDSP), through instruction by the Transporters will put in place a legal framework with the PCWs before access is granted.

We support the CMA Order and the principle of providing industry data to PCWs, to enable more frequent and improved customer switching journeys. The ICO letter to the CMA, states access to customer data must "be balanced with safeguards to ensure the personal data is kept secure and used appropriately". "Consideration therefore needs to be given to how to monitor PCWs' access and usage".

The original proposal, Modification 0593 was sent back by Ofgem following concerns PCW access and usage of DES was not robustly monitored, controlled or auditable. This appeared to place the DES solution in breach of the Data Protection Act (DPA) and risked customer data breaches. Part of the remedy is for adequate controls to be developed, so industry data could be appropriately shared with PCWs.

Modification 0593 was replaced by a variation request that amended the modification solution. This resulted in Modification 0593V being a permissions (to access data) proposal and circumnavigates the solution design and DPA compliance issues. Notwithstanding this the ICO's response to the disclosure of data to PCWs is very clear; the data is personal and therefore the safeguards of the DPA apply, so any measures the gas industry adopt need to follow the guidance given, particularly around access to data, onward disclosure and the relevant consent the PCW will need to evidence to confirm it had customer authority to access their data.

Through workgroup discussions is appears some parties want to progress the permissions modification without recognition of the DPA concerns. It should be noted a data controller is the 'person' who either alone or jointly, determines the purposes for which and the manner in which any personal data are, or are to be, processed. A data controller must be a 'person' recognised in law, so individuals, organisations and other corporate and unincorporated bodies of persons. There's something called a joint data controller where two parties process the same personal data, but that data is used for different purposes. This rule clearly extends to the Meter Point Reference Number (MPRN) data item, which both Transporters and shippers use to identify customers. Therefore our conclusion is that both Transporters and shippers are data owners and therefore both parties need to ensure the permissions modification which gives PCWs access to data and the technical solution is compliant with DPA legislation.

To progress the modification and the solution the CDSP undertook a Privacy Impact Assessment (PIA) which sets out DPA risks and what measures will be implemented to ensure system controls, adequate monitor and controls, and appropriate data access and usage. The PIA does not specify 'how' the system will monitor and control access and usage. The CDSP seeks to address the 'how' through the *PCW access to data Solution description for Modification 0593 and 095 workgroups document*[1]. For example Section 4 provides detail of how an Application Protocol Interface (API) solution can limit and control PCW access to specific data sets and access will be via secure key connections. Contracts and audits will place a framework on PCWs for access criteria and to monitor compliance.

Our main concern with the CDSP approach was that the document did not provide enough detail on how the system solution will in real time monitor and control customer data. Within the electricity solution monitoring and control has helped contain DPA breaches in real time. We expect the same or higher controls for the gas PCW solution. Anything less will be a retrograde step. Section 4.2.2 sets out inappropriate access is controlled through pre-configured bands and user performance monitoring, so that DPA breaches and inappropriate behaviour is detected early on and therefore accounts accessing customer data can be suspended. This should help to protect customer data and be an improvement compared with the previous DES solution.

Providing the CDSP delivers a technical solution that is in line with, or above the documented solution criteria, we are in a position to support this modification. We have serious reservations with our support for this modification which is still reliant on our good faith and the CDSPs wiliness to implement a complaint solution that aligns to its customer's requirements.

Implementation: *What lead-time do you wish to see prior to implementation and why?*

Given the perpetual DPA concerns and to mitigate the risk of customer data breaches, we believe the UNC permissions modification implementation date should be linked to the CDSP DSC approved solution date (tbc). This alignment should not be to the detriment to PCWs, as they have no solution to utilise, but should help ensure the CDSP delivers a robust solution that all parties are satisfied with and ensures all DPA concerns are resolved. Otherwise our fear is shippers and other CDSP customers have very little control over the final CDSP delivered solution.

[1] https://www.gasgovernance.co.uk/sites/default/files/ggf/page/2017-08/Modification%200593-095%20-%20Solution%20Description%20V2.0.pdf

Impacts and Costs: *What analysis, development and ongoing costs would you face?*

This modification addresses the permission to release data to PCWs only, so costs should be limited to Transporter and CDSP Legal costs.

It should be noted that the technical solution costs have not been so well defined. Depending on who has been asked the question at Xoserve the response has differed. Sometimes the Transporter/CDSP obligation is funded by Transporters only, sometimes Transporter and shipper funded. The cost split of the latter remains unclear and we would appreciate clear documentation from the CDSP to clarify project milestone costs, total costs and party contribution. We look forward to receiving that documented information.

Legal Text: *Are you satisfied that the legal text will deliver the intent of the Solution?*

We believe the Legal Text aligns and delivers the modification solution.

Modification Panel Members have requested that the following questions are addressed:

Q1: To inform Panel's consideration of the varied modification, views are requested as to whether you agree that Ofgem's sendback questions have been addressed in the revised modification.

The Ofgem questions and our answers are detailed below -

Q1) whether shippers and suppliers are data controllers in this context and the implications of this for data disclosure as well as any mitigating actions that should be taken,

As above a data controller must be a 'person' recognised in law, so individuals, organisations and other corporate and unincorporated bodies of persons. There's something called a joint data controller where two parties process the same personal data, but that data is used for different purposes. This rule clearly extends to the Meter Point Reference Number (MPRN) data item, which both Transporter and shipper (and supplier) parties use to identify customers. Therefore our conclusion is that both Transporters and shippers are data owners and therefore both parties need to ensure the solution is compliant with DPA legislation.

Q2) how PCWs and TPIs will have their access to data restricted (contractually or otherwise), including for access to non-domestic supply point data which is not permitted by the proposed modifications,

Not having access and not being signatories to individual Transporter/PCW contracts we are not best placed to answer this question. We trust Transporters will provide detail and reassurances to the question.

We note that the API solution should enable PCWs access and restrict access to the defined data items, whilst also restricting access to domestic only data. Given the technical solution is lagging so far behind the contractual solution, it is unclear at present how we can be sure the CDSP will build a compliant technical solution.

Further to the above we raise the point the CDSP was comfortable implementing the DES non-compliant solution, because as the data processor, the DPA risk sat with its 80 odd customers, who are data processors. This raises serious concerns with the CDSPs approach to the DPA and understanding its customer's requirements. We believe cultural

change is taking place and is driving a more customer centric provider, but culture takes time and senior management's willingness to implement.

Q3) what provisions are in place to ensure consumer consent will be positive informed consent, and

We have requested confirmation from the CDSP on this subject. The response is it will be part of the legal framework and the consent obligation will sit with the PCWs. Auditing should also enable Transporters to review PCW activity and compliance with the requirement. Whilst we accept this, we note the API solution with PCWs should also be able to validate the PCW customer interface and ensure consumer consent is in place before customer data access. This is not part of the CDSPs defined solution. We will seek to work with the industry to ensure the technical solution ensures consumer consent.

Q4) any implications and mitigating actions that should be taken in the context of the changes to Xoserve's governance and funding arrangements as a result of FGO and the forthcoming implementation of the GDPR.

The new governance arrangements are still bedding in. Whilst in the main, the co-operative model is a success, with all industry parties having much more control over their Provider and the Provider making changes to be more customer focused, we remain concerned by the observed lack of internal governance at Xoserve and decisions made by them, which could be to the detriment of the CDSP's customers.

Given the persistent DPA concerns and the pivotal role the CDSP has in managing customer data, we are surprised by how low their DPA standards and controls appear. We are also alarmed by how light their DPA knowledge appears to be within the organisation. Addressing these concerns could go some way to managing Xoserve's GDPR implementation.

Are there any errors or omissions in this Modification Report that you think should be taken into account? *Include details of any impacts/costs to your organisation that are directly related to this.*

None identified

Please provide below any additional analysis or information to support your representation

N/A