Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to the CMA's call for representations on the following CMA Energy Market Investigation Orders:

1. **Energy Market Investigation (Database) Order 2016**
2. **Energy Market Investigation (ECOES/DES) Order 2016**
3. **Energy Market Investigation (Gas Settlement) Order 2016**

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Information Commissioner welcomes the opportunity to respond to the CMA's consultation on the remedies arising from the Energy Markets Investigation (EMI). Her response is focussed on the areas where the remedies most impact on individuals' privacy and associated rights.

The Commissioner recognises the value of improved competition within the energy sector, but considers this must not be achieved at the expense of individuals' rights. Consumer trust and confidence are essential to ensuring a competitive market, and care should be taken to ensure this is not undermined by well-intentioned measures that could have adverse impacts. As the CMA's recent study into the commercial use of consumer data[1] identified, consumer trust and confidence in the use of their data could be fragile and at risk – and any steps taken in the energy sector must not further compromise that trust and confidence.

The ICO's 2016 annual track survey showed that consumers fear their data being sold for third party marketing purposes almost as much as

[1] CMA "The commercial use of consumer data", June 2015: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

they fear it being stolen[2]. There is a risk that extensive, invasive or unnecessary processing of personal data for direct marketing purposes could damage levels of consumer trust in the energy market.

The Commissioner believes that individuals' choices in terms of their personal data should be respected to ensure trust is not eroded and that the positive work undertaken in relation to smart metering - such as the privacy-respecting options set out within the Data Access Privacy Framework - is not undermined.

The protection of personal data and respect for private and family life are fundamental rights afforded to UK citizens[3]. The CMA's proposals, which could see the sharing of personal data in ways not envisaged and contrary to individuals' clearly expressed wishes, engages those rights. It is noted that the Digital Economy Bill is currently undergoing scrutiny in Parliament, and that some of the provisions relating to data sharing have raised significant concerns by parliamentarians.

1. Energy Market Investigation (Database) Order 2016 ('the Database Order')

Of the published Orders, the Database Order raises the most potential data protection and privacy concerns as it represents the greatest intrusion on individuals' privacy. This is because it may result in individuals' marketing preferences – and wider energy choices – being overridden should those individuals fit within certain criteria.

It is understood the overriding purpose of the Database Order is to stimulate customers who have been on their suppliers' standard variable tariff (SVT) – a default, expensive tariff – for more than 3 years, to change tariff and/or supplier to get a better energy deal. The terms 'sticky customer base' and 'Disengaged Customers' are respectively used in the EMI and draft Database Order.

The EMI Final Report noted that those falling within the category of 'Disengaged Customers' represent approximately 55% of the overall energy market, which means those affected will number in the millions[4]. Given the number of individuals who may be affected, any remedy needs to be carefully considered in order to avoid generating complaints and hampering the ability of those concerned – including the Information Commissioner's Office - to effectively deal with these.

[2] ICO Annual Track 2016: annually commissioned research to snapshot public knowledge and feelings about information rights law and issues: https://ico.org.uk/media/about-the-ico/documents/1624382/ico-annual-track-2016.pptx

[3] Articles 7-8, EU Charter of Fundamental Rights; Article 8, European Convention on Human Rights

[4] We note that the EMI Final Report references the largest number of affected customers as being potentially in excess of 10 million across the market.

It is understood that the key approach identified by the CMA to tackle the 'sticky customer base' is to increase the level of promotional and marketing material received by those customers in the post. There is a fundamental issue regarding fairness to be considered here. The DPA requires that processing of personal data must be undertaken fairly, and that individuals should know what their data will be used for. Is what is being proposed within individuals' reasonable expectations? Is it objectionable in its own right? The issue of fairness is challenging in the context of direct marketing as individuals may have strong feelings about unsolicited marketing - no matter how beneficial a public body considers that marketing to be. It is possible that despite a scheme being lawful it may still raise significant concerns amongst the general public with respect to how their data has been used. This could lead to poor outcomes.

It is noted that the CMA's Database Order requires energy suppliers to identify 'Disengaged Customers' according to the criteria set by the CMA, and to then send a postal 'First Contact Communication' informing the customer that they are paying too much for their energy and that better deals may be available. The letter is to include an opt-out opportunity, as well as explaining that if the customer does not actively opt out their data will be passed to Ofgem.

The data to be shared is significant, including account holder name and postal address, address of the meter (if different), meter point access number (MPAN), tariff name and details, and details of energy usage. It is understood that that the categories have been selected to enable rival suppliers to provide a relevant quote.

Once the data has passed to Ofgem there are several possible options, namely: (i) rival suppliers would be able to access the data and to send their best offer to the customer directly by post; or (ii) Ofgem would collate multiple best offers and share these with the customers in a single postal communication under the guise of a 'trusted voice'.

It is understood both options are currently being trialled on a small scale - along with a control group who will not receive mail contact in this way - and the ICO is extremely interested to learn the outcomes of these trials. It noted that a significant proportion of the detail relating to these proposals has yet to be finalised (to include frequency of contact; any limitations on the number of rival suppliers who can access the data and contact the customers; how long the data can be retained for; whether the contacts will be sent from the centralised database or whether the data will actually be drawn down from the database into the rival suppliers' systems; to name but a few).

If the CMA decides to continue with the proposed approach the Information Commissioner has a strong preference for the second of these options, namely Ofgem assumes the role of a 'trusted voice' and sends a summary of the best price tariffs offered by rival suppliers to the customer.

There are a number of powerful arguments in favour of this 'trusted voice' approach:

- **minimisation of information risk** – the risk of proliferation and duplication of customer data (accurate or otherwise) is significantly reduced as the data will stay with the one party. Restricting the spread of customer data is an important factor in ensuring customers can remain in control of their data;

- **the ability for Ofgem to police and control access to the customers** – which will help avoid the risk of individuals receiving a bombardment of marketing. We understand there are currently in excess of 40 energy suppliers, and should each supplier be given the ability to send a customer even one postal communication the level of contact could be overwhelming and unwarranted;

- **Ofgem can control the acquiring of best offers, and can restrict the information which needs to be provided to rival suppliers in order to obtain quotes -** we can see that positive data protection measures could be used to protect customers' data here, for example Ofgem could provide the data to rival suppliers in a hashed, suitably anonymised format to ensure accurate and unbiased quotes are returned;

- **ease of managing customers' opt out requests once their data has passed into the database -** unlike the rival supplier model, the trusted voice approach makes opting out significantly easier for all concerned, and is likely to be actioned more promptly and effectively; and

- **Ofgem have the data needed to establish how effective the scheme is** (and/or the level of complaints that it is generating).

There are a number of other specific data protection issues and concerns which are raised separately in the following paragraphs.

The Commissioner's aim is to ensure that any remedy implemented by the CMA complies with requirements of the DPA, anticipates the forthcoming General Data Protection Regulation (GDPR)[5] and respects individuals' rights whilst increasing competition in the market. The ICO

[5] Currently in force, but the provisions take effect as of 25 May 2018.

continues to offer advice and guidance to both the CMA and Ofgem as they explore different approaches to implementing the proposed remedy.

It is important to consider other less privacy intrusive options to the fullest extent possible. For example, it may be possible for suppliers to mail existing customers with their rival suppliers' offers, or to make the use of digital comparison tools easier and quicker for consumers to use; the work being undertaken by banks to develop open APIs in response to the CMA's market study into retail banking is noted in particular.

1.1 Right to prevent processing for the purposes of direct marketing – section 11 of the DPA

Section 11 of the DPA states that:

> *"An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject."*

The right under Section 11 is a powerful one, and it is the only right in the DPA that is an absolute right and not subject to any exemption. An organisation in receipt of a Section 11 notice should ensure that not only does it avoid sending direct marketing to the individual concerned, but that it does not share or sell that individual's personal data to third parties for the third party's direct marketing purposes.

The Information Commissioner is especially concerned to ensure that any remedy implemented by Ofgem and the CMA respects this right. It is understood that at present the intention is for the First Contact Communication to be sent and the customers' data passed to the Ofgem database, irrespective of whether a preference has been expressed by the customer to not receive direct marketing. Customers who have taken the time to express a preference about marketing communications should have that preference respected.

Irrespective of the wider point about the use of the data for marketing purposes down the chain i.e. once the data has passed to Ofgem, and then potentially on to rival suppliers, it is our view that the First Contact Communication could itself constitute direct marketing depending on how it is conveyed. The definition of direct marketing included in the DPA is the "communication (by whatever means) of any advertising or marketing material which is directed to particular individuals", and this has been construed broadly to include the promotion of not only goods and services

but also of aims and ideals[6]. In order to avoid being classified as 'direct marketing' the content of the First Contact Communication would need to be neutral and informative, and not promote any particular service or seek to raise any particular party's profile. It is accepted that this is challenging to achieve in practice given the nature of the communication, but nonetheless it is a matter that Ofgem and the parties concerned need to work towards.

Any decision to override individuals' wishes could also impact on the availability of a condition for processing under Schedule 2 of the DPA[7]. It is understood that should the rival supplier contact model be used, the intention is to rely upon the 'legitimate interests' condition as the legal basis for the processing. This condition requires a careful balancing of the data controller's interests against the unwarranted prejudice to the rights and freedoms or legitimate interests of the individual concerned. It seems unlikely that in cases where an individual has expressed their wish to not receive direct marketing in accordance with their rights under the DPA, that the legitimate interests condition could safely be relied upon as an appropriate condition for processing the data.

1.2 Sensitive personal data

From briefings received about the Database Order, it is understood that the initial intention was that sensitive personal data would not be shared. It is the Information Commissioner's concern, however, that the remedy cannot be effectively implemented without sharing some sensitive personal data. This is because a significant proportion of the customers who fall into the category of 'Disengaged Customers' may be identified as vulnerable in some way or have accessibility or contact requirements. Some affected customers may also be on tariffs which reveal additional information about them, such as recipients of the Warmer Homes Discount.

The DPA requires data to be adequate for the purpose(s) for which it is being processed. To implement a remedy that required individuals to be contacted via post, but did not take account of, for example, visual needs of the customer would not accord with requirements of the DPA. The sharing of sensitive personal data would need both a Schedule 2 and a Schedule 3 condition to meet the requirements of the first principle. This would be challenging in the circumstances and the CMA will need to give

[6] To include promotion of, for example, political aims and ideals – as endorsed by the Information Tribunal's decision relating to the Scottish National Party making automated calls in Scotland to promote recipients voting for them. The decision found that the Privacy and Electronic Communications Regulations 2003 – which set rules for the use of unsolicited direct marketing by electronic means - do apply to political parties: http://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i111/SNP.pdf

[7] Principle 1 requires that personal data is processed fairly, lawfully and in compliance with one or more conditions for processing – which are accepted justifications for processing personal data set out in Schedule 2 of the DPA. Where sensitive personal data is to be processed (data about race/ethnicity, health, trade union membership, sex life, political opinions, religious beliefs or alleged/actual criminal activity) an additional condition for processing must also be met from Schedule 3 of the DPA.

careful consideration to this point. It is worth noting, in particular, that the legitimate interests condition is not available for the processing of sensitive personal data.

1.4 Practicalities

There are a number of practicalities which need to be considered, whichever version of the remedy is taken forward:

- **Security of the database -** any database needs to be sufficiently secure in accordance with the requirements of principle 7 of the DPA. In particular, detailed consideration needs to be given to access controls to ensure these are sufficiently robust. There is the potential for a large scale database of vulnerable individuals to be created, and any security measures must take account of the likely appeal such a database would have for malicious or criminal actors;

- **Onward usage provisions** – should the rival supplier model be adopted, clear and careful thought would need to be given to how to ensure that data is not used for additional purposes, and is not cross-referenced with existing datasets to create enriched data. Similarly, the need to ensure that the database itself is not seen as a useful resource for other purposes and used outside the initial purposes for which it was collected is important;

- **Access revocation provisions** – and how infringements of the access requirements will be identified;

- **Preventing duplication and proliferation of personal data if the rival supplier/multi-party model is adopted** – with particular attention needed as to how accuracy will be ensured across the piece;

- **Ensuring customers actually receive the First Contact Communication** and therefore have the opportunity to opt out;

- **How opt outs from the database would be managed if the multi-party/rival supplier model is used** as the opt out would need to be practically reflected across multiple parties;

- **How to make it clear what the opt-outs relate to** - an initial opt-out in response to the First Contact Communication would be an opt-out from both data being passed to the database *and* also from receipt of marketing communications. An opt-out sent subsequent to a customer's data being shared with the database is an opt-out from receipt of communications. It should be considered whether the latter also necessitates deletion of the data from the database.

Finally, it is our view that if a customer opts out in response to the First Contact Communication, their data should not then be shared with the database at all. Customers would not expect their data to be shared for, for example, monitoring of the success of the scheme and it could well be excessive and unnecessary to do so.

2. Energy Market Investigation (ECOES/DES) Order 2016 (the ECOES Order)

The ICO provided comments on enabling price comparison websites (PCWs) to access the ECOES and DES databases at the proposal stage, and concerns were identified in relation to ensuring any such access is undertaken in compliance with the requirements of the DPA[8].

The Order provides for PCWs to be able to access certain meter data in order to enable consumers to switch between suppliers more easily. The ICO's position remains unchanged: the potential benefit of improved ease of access for consumers to competitive energy deals via PCWs needs to be balanced carefully with appropriate safeguards. The Order makes clear that access must be provided by MRASCo[9] to PCWs following written request and subject to "reasonable access conditions". Presumably, the written request is to originate from each individual PCW, but this is not clear from the way in which the Order is currently worded.

No detail is given as to what would constitute "reasonable access conditions", and the term is not defined. Careful thought needs to be given to the criteria used to enable access, as it is understood that PCWs and energy suppliers are not subject to equivalent sectoral regulation. If data is moving from a more stringent regulatory environment to a less stringent one, then care needs to be taken to ensure that this does not expose the data to unnecessary risk or leave consumers without control or recourse.

The Order addresses the high level principle of enabling and requiring MRASCo to provide access to PCWs. Any such access needs to be balanced with safeguards to ensure the personal data is kept secure and used appropriately. We would expect any subsequent guidelines, rules or regulatory framework governing this access to address the following:

- The ability for access to both ECOES and DES to be removed should a PCW be found to be using that access mechanism, or the data

[8] ICO response to the CMA's "Energy Markets Investigation: notice of possible remedies" paper https://ico.org.uk/media/about-the-ico/consultation-responses/2015/1432296/ico-response-to-energy-market-investigation-notice-of-possible-remedies-20150803.pdf

[9] MRASCo is the company that administers the Master Register Agreement – the industry-wide agreement that provides a governance mechanism to manage the processes established between electricity suppliers and distribution companies to enable electricity suppliers to transfer customers.

obtained, inappropriately. Consideration therefore needs to be given to how to monitor PCWs' access and usage;

- As noted in the ICO's previous response on PCW access to ECOES and DES[10], the data within those databases constitutes personal data. This means that any PCW accessing this data would need to comply with the DPA in doing so – including meeting a condition for processing under Schedule 2 of the DPA. Our previously stated view is that the only condition likely to be available is consent – that is, the PCW will need to obtain an individual's consent to access their ECOES/DES data at the time they sign up to the price comparison/switching service. Thought should also be given to ensuring that the high standard of consent under the GDPR can be met, and that the consent can be withdrawn at any time;

- Record-keeping in terms of consent. The GDPR requires data controllers (such as PCWs and energy suppliers) to be able to demonstrate an individual has given their consent. PCWs should be required to keep such records; and

- Retention and deletion. Principle 5 requires that personal data is not kept for longer than necessary for the purpose for which it was obtained (and this is also reflected within the GDPR). Any personal data collected must be subject to strict retention and deletion policies, and, should PCWs be found to be exceeding or disregarding such policies, this should be a factor which would enable their access to the data to be withdrawn.

3. Energy Market Investigation (Gas Settlement) Order 2016

It is understood that the purpose of this Order is to facilitate improved reconciliation of gas charges across the sector to reduce costs, with the intention of reducing charges to customers over time by increasing efficiencies in the market. To achieve this, there is a need for suppliers to be able to access more frequent meter readings than have previously.

It is important that any access regime aligns and is consistent with the access regime set out in the smart metering framework's Data Access and Privacy Framework (DAPF) insofar as possible to avoid confusion and potential unfairness. The DAPF regime enables individuals to exercise control over the use and collection of their data whilst facilitating billing.

Whether there is anything additional which suppliers need to do under the DPA in respect of the Order's new requirement is dependent upon what

[10] ICO response to the CMA's "Energy Markets Investigation: notice of possible remedies" paper https://ico.org.uk/media/about-the-ico/consultation-responses/2015/1432296/ico-response-to-energy-market-investigation-notice-of-possible-remedies-20150803.pdf

customers are already aware is taking place. If additional data is to be collected, if data is being used for new/different purposes or if the increasing granularity of collection means that more information could be deduced from the information, then appropriate notice needs to be given to the customers to comply with the requirements of fairness under principle 1 of the DPA. If individuals have taken steps to exercise control over the use and collection of their data, those wishes should not be overridden.

Finally, any data collected as a result of this requirement should only be used for this purpose. It should not, for example, be used for other purposes such as targeting marketing or promoting different tariffs to individuals.

The Information Commissioner reiterates the fact that she continues to offer support to the CMA, Ofgem and sector more generally in ensuring that any competition remedies are implemented in a privacy-friendly way that respects individuals' rights and builds consumer trust and confidence.

November 2016