The Information Commissioner's response to the Department for Business, Energy and Industrial Strategy call for evidence on implementing Midata in the energy sector

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's fundamental objective during her 5-year term is to build a culture of data confidence in the UK, helping our digital economy to grow in a strong and sustainable way. In order to achieve this objective it is essential that government builds privacy into the development of public policy. It should not be a case of privacy *or* innovation, but privacy *and* innovation.

The Commissioner welcomes the opportunity to respond to this call for evidence on implementing Midata in the energy sector. The Commissioner is supportive of initiatives that provide individuals with access and control over the information organisations hold about them, and which allow that information to be utilised in beneficial ways. The call for evidence, however, raises a number of important issues that should be considered by the Government before commencing the relevant provisions of the Enterprise and Regulatory Reform Act (ERRA).

The Information Commissioner's Office has provided advice and guidance to the Government on the Midata programme over a number of years. We have continuously submitted that building and maintaining consumer trust is of central importance in ensuring the success of any scheme. Building consumer trust and ensuring that it is not lost or eroded should be a central concern for BEIS as it seeks to implement this policy.

Our most recent annual track survey in 2016 found that only 1 in 4 adults trust business with their personal information. Energy companies fared slightly better than average with a third being trusted whereas internet brands were the least trusted (22%).[1] The research also found that trust in the use of personal data is essential for businesses pursuing data driven business models.

[1] https://ico.org.uk/media/about-the-ico/documents/1624382/ico-annual-track-2016.pptx

In 2015 the Competition and Markets Authority published its call for information on the commercial use of consumer data[2] and identified potential barriers to consumers trusting firms, namely that consumers lack awareness and understanding, and they are concerned about the sharing of their data. The CMA reported that they had found "widespread concerns about the effectiveness of the means by which consumers engage with the process of collecting data… …[and] the evidence suggests many consumers do not actively engage with these mechanisms and, where they do, they are not always sure what they are agreeing to.".

In 2015 the Citizens' Advice Bureau published its report *Personal data empowerment: time for a fairer deal?*[3] which sought to "articulate a fresh vision of personal data empowerment: one that sees the value of data shared more evenly amongst both the consumers who generate data and the organisations that use it; one that balances safeguards with the ability to innovate and one that contributes to a more stable personal data ecosystem that better serves consumers in the 21st century.". The report advocated 'personal data empowerment' as a means of achieving this, namely giving consumers meaningful control over their personal data in order that they can easily understand how it is used and the benefits arising from it, all with appropriate trust mechanisms.

Legislation and regulatory requirements have an important role in creating the infrastructure and ecosystem that will help to build trust. Whilst data protection law has an important role in helping build that ecosystem it is not the only determining factor, and Government should ensure that it doesn't place undue reliance on it to deliver its desired outcomes.

The Information Commissioner notes the differing approach being contemplated by BEIS in the call for evidence, compared to that which is being adopted by HM Treasury in relation to the retail banks who are being subjected to similar measures, also by way of a CMA competition remedy. As a precursor to the CMA's Order being made, the Treasury and the Cabinet Office commissioned Fingleton Associates and the Open Data Institute to write a report on the benefits and challenges associated with open banking[4]. Further work was undertaken by industry through the Open Banking Working Group on the implications[5]. The banks affected by the CMA Order have now been obliged to establish an implementation entity steering group (IESG) and to appoint a trustee to oversee implementation[6]. The Information Commissioner suggests that it would be beneficial for BEIS to take into account the issues identified by

---

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

[3] https://www.citizensadvice.org.uk/Global/Public/Corporate%20content/Publications/Personal%20data%20empowerment%20report.pdf

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF

[5] Further information at http://theodi.org/open-banking-standard

[6] See http://www.paymentsuk.org.uk/policy/payments-CMA-remedy-phase1/temporary for further information about the work of the IESG

the banking industry, and to build upon the work undertaken by the Treasury, Cabinet Office and banking industry already.

Government should also consider that as of 25th May 2018 data controllers operating in the energy industry will be subject to the data portability provisions of the General Data Protection Regulation (GDPR)[7]. In summary, Article 20 provides that individuals have the right to receive personal data about them in a structured, commonly-used and machine readable format, and they have the right to transmit the data between organisations without hindrance. Where technically feasible, individuals will have the right for the data to be directly transmitted from one organisation to another. The intention of this right is to make it easier for the customers of energy companies, for example, to transfer certain account information from one provider directly to another to facilitate a change of provider. Clearly there is a considerable overlap between data portability under GDPR and Midata under ERRA.

The Article 29 Working Party[8] has recently adopted an opinion on the right to data portability[9] and this explains that the scope of the portability right is wide and includes the personal data generated by, and collected from, the activities of users - such as raw data generated by a smart meter. The Working Party has stated that it strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability. Clearly, governments and regulators have an important role to play too.

Energy suppliers will need to comply with GDPR in just over 15 months' time. We are currently in the transitional period during which time energy companies ought to be working towards implementing GDPR provisions, including those relating to data portability, into their businesses. BEIS should carefully consider the interaction between ERRA and GDPR requirements. In light of this analysis, Government may consider that the Midata provisions, in practical terms, will be short-lived and significantly overlap with the data portability requirements.

In any event, BEIS should consider how we can best work together - with Ofgem - to ensure the energy industry delivers data portability rights under GDPR in ways that meet the Government's desired outcomes for energy customers.

[7] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of personal data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[8] The pan-European organisation of data protection authorities established under Article 29 of the Data Protection Directive, and which will form into the European Data Protection Board under GDPR

[9] http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf and http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf

Question 1: Do you agree that API access for TPIs should be available on an 'access by default' basis? Do you have any evidence that such an approach could cause customer detriment? If so, please provide details.

Question 2: Do you agree that Government should provide energy suppliers some flexibility about how to apply conditions on authorising access to customer's data? If you do not agree, please give reasons and suggest an alternative proposal.

As noted above, the data portability requirements will apply to energy suppliers from 25 May 2018. Individuals' rights under Article 20 are broad; there is no provision for a supplier to restrict transfers of data between particular Third Party Intermediaries (TPIs) or categories of TPI. The decision to port data is a matter for the individual to determine; to whom it is ported is not necessarily a matter for the energy supplier to be concerned with.

There is, however, clearly an imperative to build consumer trust and Government should consider how it can help consumers make good choices about the TPIs they interact and share data with. Consideration should also be given to how concerns about the handling of data by TPIs are identified and brought to the attention of the ICO, other regulators and the public.

Question 3: Do you agree that customers should have the choice between providing consent to a third party to access their Midata on a one off, time-limited basis and annual or ongoing basis?

Question 4: Do you agree that for one off access 30 minutes is an appropriate consent period? Please provide details.

Question 5: Do you think that longer access periods should be for one year or ongoing subject to customers opting out? Please provide details.

The ICO will shortly be publishing guidance on consent under the GDPR, which is set at a high standard: "freely given, specific, informed and unambiguous". Individuals should be able to withdraw their consent at any time, and it should be as easy to withdraw the consent as it is to give it. It should be noted that the GDPR does not specify the frequency or duration of consent, but in terms of consent needing to be 'specific' being clear about time limits will go towards achieving that element.

It's important from a user experience perspective that the customer journey is not unduly interrupted through a need to seek fresh consents unnecessarily often. Seeking consent is, however, an important way in which individuals can exercise control over how their data is used and shared. In general terms, consent that is granted on an ongoing basis is problematic, as it risks the consent degrading below the threshold over time; individuals may not remember they have given their consent if it was sought too long ago, and therefore they may be unable to exercise any control to remove it and it may no longer meet the high threshold of consent. However, this is less of an issue where the processing of personal data, eg its use or disclosure, does not change during the period following the obtaining of consent. An alternative may be to consider

mandating a requirement to somehow periodically remind individuals that they have a right to withdraw their consent and provide an easy mechanism to achieve that.

In terms of whether 30 minutes is an appropriate period for one-off access, consideration should be given to the risks associated with adopting this time period. Needless to say, access should be given for no longer than is necessary and this will be determined by operational factors.

Question 6: Do you agree that all customers, including those without an online account, should be able to grant Third party access to their data?

The rights under GDPR are not restricted to those individuals who have an online account with a supplier; it is not the case that individuals *should* be able to grant third party access but that they have a *legal right* to grant third party access to the data where it is technically feasible. That being the case, we suggest that all customers, regardless of whether they have an online account, should be able to grant third party access to their data. There are clearly challenges to be overcome in terms of customer verification to prevent unauthorised access to the data, and to address any related security concerns.

Question 7: Is there a minimum number and/or combination of data fields needed to verify a customer is legitimate and if so, which data fields would be appropriate for this function?

This is a matter for suppliers to determine.

Question 8: Do you agree that the following data fields should be added to the API specification: meter type, Warm Home Discount Indicator, consumption data by time of use for those customers on Economy 7 or other time-of-use tariff? Question 9: Should additional data fields be introduced from the start of the mandatory Midata implementation or phased in over time? If you think they should be phased in, how and when should this be done?

Only data fields that are relevant ought to be included in the specification. If those items are relevant for the purposes of performing a comparison and for switching energy provider then they ought to be included in the specification. It's important that individuals should be afforded sufficient control over the items of data that they share, and that it should not be an "all or nothing" proposition ie the customer should be able to choose whether they share their warm home energy discount status or not.

Question 10: Should Government follow a collaborative process with stakeholders if changes to the technical specification need to be made?

It's important that the specification is capable of being amended to take into account any developments. A collaborative approach with industry is a reasonable approach to take in this context.

Question 11: Do you agree that existing data protection legislation is sufficient

to deal with customers' energy Midata. If not, provide evidence and a proposal for how additional protections could work.

As set out above, data protection law provides for robust safeguards and the Information Commissioner has a range of enforcement powers to deal with the misuse of data by suppliers and TPIs. It should be noted that the Commissioner does not have any powers under ERRA to require suppliers to build the necessary infrastructure and release the data in question – although she does, of course, have a regulatory power over the processing of personal data that occurs under ERRA. If parallel requirements are placed on industry so that they have to comply with both ERRA and GDPR portability this could create overlap between the respective regimes. This should be avoided as far as possible, not least in the interests of consumer transparency and control.

Question 12: Do you agree that Ofgem is the most appropriate organisation to carry out monitoring and enforcement of fulfilment of Midata requests? If not, which organisation would be preferable and why?

Question 13: Do you agree with the enforcement regime overseen by Ofgem would be the most appropriate way to deal with breaches of Regulations requiring suppliers to provide customer data? If not, can you propose an alternative and say why this would be more appropriate.

The supervisory authority under GDPR will be the Information Commissioner's Office. Taking into account the time to commence ERRA, and allowing sufficient time for industry to build and implement the necessary infrastructure, it may be that the enforcement regime will only apply for a very short time.

The ICO is deeply committed to working closely with other regulators, such as Ofgem, to ensure wider aspects of the data protection regime reflect their regulatory interests and concerns. Our mutual interest should be to provide a seamless protection system and reliable choice mechanism to consumers. It is especially important that the ICO and Ofgem work together to leverage our joint influence to ensure that industry delivers data portability in a way that provides consumers with tangible ways in which they can easily use their data, and which facilitates competitive markets.

Question 14: Do you think that quality assurance of Midata needs to be undertaken/ If so, how would this be best achieved?

The Information Commissioner is supportive of initiatives that help organisations ensure the data they hold is accurate. The DPA and the GDPR both contain provisions relating to the accuracy of data.

Question 15: Are there aspects of the wider Midata programme that we should take into account when developing Regulations in the energy sector to maximise the benefits of the wider programme for customers?

BEIS should engage with the Competition and Markets Authority's study into digital comparison tools to ensure that any regulations developed help to address any concerns that the CMA may identify.

Question 16: Are you aware of any evidence available from other countries that have implemented similar proposals? If so, can you provide details on customer benefits?

No.

Question 17: Do you agree that energy suppliers with fewer than 50,000 customers for a given fuel should be exempt from this regulation?

No. The right to data portability will apply in any event to those firms.

Question 18: In view of the work already undertaken and the recommendation of the CMA, are there any further issues to consider with regard to when these proposals should be implemented?

No.

Questions 19 to 31 relate to cost impacts which we are not in a position to respond to.

Information Commissioner's Office
February 2017