The Information Commissioner's response to the Ofgem consultation Standards of Conduct for suppliers in the retail energy market

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Privacy and Electronic Communications Regulations 2003 (PECR), the Freedom of Information Act 2000 (FOIA), and the Environmental Information Regulations. 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 Ofcom's consultation on changing the regulatory rules governing communications providers.

It should be noted that data protection laws are undergoing significant reform at the present time and the General Data Protection Regulation (GDPR) will take effect in the UK from 25 May 2018. Laws concerned with electronic direct marketing are also undergoing reform and this may lead to changes to PECR. We would be happy to provide further advice and guidance to Ofgem on the potential impact of these reforms.

The DPA is concerned with the collection and use of personal data. Personal data is information that by itself, or in conjunction with other information, identifies a living individual. The DPA requires that personal data should be handled in accordance with the data protection principles. In particular, personal data should be used fairly and a key aspect of fairness is ensuring individuals are appropriately informed about how their data is used. Individuals should also be able to exercise control over their data where appropriate.

When personal data is to be used in new or novel ways an organisation may consider undertaking a Privacy Impact Assessment (PIA). A PIA will help an organisation identify, consider and address any privacy and data protection risks. Under GDPR assessments of this nature - referred to as "Data Protection Impact Assessments" - will be mandatory for particular types of high risk processing.

Organisations will also need to ensure electronic direct marketing, such as marketing by phone, fax, SMS or email, is carried out in a way that complies with PECR. Marketing is defined widely and includes an activity to promote a product, service, aim or ideal.

The Commissioner's response to this consultation is restricted to those questions falling within the ICO's role as the UK's independent authority set up to uphold information rights in the public interest and to promote data privacy for individuals. She would be happy to provide Ofgem with further advice or assistance on the data protection implications of these proposals, if needed.

Question 6: Do you support our proposal to introduce a broad "informed choices" principle into the domestic Standards of Conduct?

The Commissioner considers that individuals should be fully informed in order that they can freely make the best choices for themselves. However, there are some practical concerns about marketing that she considers are worthy of further consideration and clarification.

The ICO Direct Marketing Guidance makes it clear that 'marketing' is an activity to promote products, services, aims or ideals. It is unclear whether the 'informed choices' principle includes a requirement to market to consumers, or is simply setting out good practice requirements.

PECR sets out rules that organisations must comply with when undertaking direct marketing by electronic means such as telephone calls, text messages, emails and faxes. Any electronic marketing activity must comply with the provisions of PECR.

PECR does not cover postal marketing. However, under the DPA, individuals can make a written request to an organisation that their data is not used for direct marketing purposes. Organisations are unable to refuse a request. Where an organisation has received a written request, including email requests, that they not be sent direct marketing, that organisation must comply.

If there is an intention to introduce a marketing requirement, there should be a clear statement that this should not override individuals' data protection rights.

Question 10: Do you agree with our proposal to include a broad vulnerability principle in the domestic Standards of Conduct? If not, please explain why with supporting evidence.

The Commissioner agrees that the needs of individuals in vulnerable circumstances should be taken in to account. Data protection law places duties on organisations to handle personal data appropriately and these should be taken into account. These duties include having a legal basis to handle the data, making sure that individuals understand how and why their data is being handled, and that they only hold the minimum amount of data necessary.

Individuals may be vulnerable for a variety of reasons. The DPA requires that personal data is processed 'fairly'. This requires that individuals understand what data is being collected and the purposes for which it will be used, as well as ensuring that the processing is not generally unfair to the individual. Organisations collecting or using personal data will need to ensure that individuals understand what will happen with their data and what purpose(s) it will be used for. In the case of people in vulnerable situations, organisations will need to carefully consider how they provide them with high-quality information. The ICO code of practice on privacy notices gives useful guidance to organisations about how to provide information to individuals.

The DPA includes particular categories of 'sensitive personal data', which are broadly similar to the 'special categories' of personal data under the forthcoming GDPR. There are more stringent protections for sensitive personal data under the DPA and GDPR. Some of the conditions under which individuals may be considered 'vulnerable', such as those relating to their physical and mental health, will be sensitive personal data for data protection purposes. It is therefore important that organisations understand what data falls within the definition of sensitive/special categories of data.

Apart from not violating other laws, organisations must also have a legal basis on which to hold and handle personal data. These are currently set out in the DPA under schedule 2 (processing personal data) and schedule 3 (processing sensitive personal data). Under the GDPR, they will fall under Article 6 (lawfulness of processing), Article 7 (conditions for consent), and Article 9 (processing of special categories of personal data).

If energy suppliers choose to rely on the explicit consent of individuals to process sensitive personal data about any vulnerability, they must ensure that it is fully informed, freely-given, and that there is a mechanism in place for individuals to withdraw consent later. The ICO recently published draft guidance on consent for consultation. The consent guidance is intended to help organisations understand what constitutes valid consent under the GDPR.

Organisations collecting and using personal data must take care not to collect data that is excessive for the purpose(s) for which they need it. In

practice, it may not be appropriate to record details of individuals' conditions if a code identifying the needs of that individual would be sufficient.

Question 11: Do you agree with our proposed definition of 'Vulnerable Situation'? If not, please explain why with supporting evidence.

It would not be appropriate for the Commissioner to determine what definition of a 'vulnerable situation' is suitable for the energy sector. The definition in the consultation is:

A Vulnerable Situation means the personal circumstances and characteristics of each Domestic Customer create a situation where he or she is:

- *Significantly less able than a typical Domestic Customer to protect or represent his or her interests; and/or*
- *Significantly more likely than a typical Domestic Customer to suffer detriment, or that detriment is more likely to be substantial.*

This does not appear to be an unreasonable definition.

We would like to note that while there are situations where vulnerable circumstances may cause a person to become disengaged, not all disengaged customers will be vulnerable.

It is unclear how energy suppliers would identify vulnerability. If a supplier intends to process personal data in order to identify individuals who may be in a vulnerable situation, then they will have to ensure that they do this in a way that complies with data protection obligations. In the case that a supplier were to want to use existing data for new purposes, individuals would have to be informed, and the supplier would need to identify its legal basis for processing the data. The supplier would typically also need to undertake a Privacy Impact Assessment (PIA). A PIA will help to identify data protection and privacy risks for both customers and organisations, and may help in developing appropriate mitigations.

Question 12: Do you have any comments on the proposal to amend SLC 5?

It is unclear whether personal data would be used to monitor compliance. If personal data would not be required, then it should not be used.

If personal data would be required, then it would need to be processed in compliance with the requirements of the DPA and GDPR. In particular, the

fairness and lawfulness requirements will need to be considered in detail. The PIA process will help to identify compliance risks when undertaking monitoring.

Question 18: Can you provide evidence of any unintended consequences that could arise as result of our proposals?

In general terms, any processing of personal data must comply with the DPA, and in future, the GDPR. PIAs can be invaluable in identifying and mitigating privacy and data protection risks. Annex one of the ICO Privacy Impact Assessments Code of Practice includes screening questions that help identify when a PIA would be helpful.

As outlined in the answer to question 6, any organisation considering marketing activity will need to comply with written requests to stop, or to not begin, using personal data for direct marketing purposes. Furthermore, any electronic marketing activity will need to comply with PECR. Consideration will also need to be given to ePrivacy Regulation which is currently being negotiated in Europe.