The Information Commissioner's response to Ofgem's Statutory Consultation: Enabling Customers to make informed choices

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 Ofgem's consultation on enabling consumers to make informed choices. She recognises the importance of empowering people to make choices based on high-quality information and the importance of ensuring the needs of vulnerable people are taken in account. The Commissioner's response is restricted to those areas that fall within her regulatory remit.

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 need to undertake a Privacy Impact Assessment (PIA). Undertaking a PIA will help an organisation identify, consider and address any privacy

and data protection risks. Under GDPR assessments of this nature 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.

Question 8: Do you consider that the proposed principles are a sensible way of achieving our policy objective?

The proposed principles appear to be a sensible way of achieving Ofgem's policy objective, however in practice organisations will have a number of important considerations to take into account when considering how to comply with those principles and their obligations under data protection law.

It is important that firms are given space to innovate but consumers' interests - and their personal data - should always be appropriately protected. Undertaking a robust Privacy Impact Assessment (PIA) should enable the identification of risks and allow for mitigating measures to be put in place. For example, we would recommend that live data sets are not used in test environments where possible and that individuals should be appropriately informed as to how their data will be used.

With regard to the proposed wording of the third principle, customers' needs, preferences and characteristics may include 'personal data' and/or 'sensitive personal data'. Sensitive personal data (under GDPR 'special categories of data') attracts more stringent protections. It will be important for organisations to ensure that only the minimum information necessary to meet customer needs is recorded, and this may take the form of a 'needs code'. Organisations must be clear about what their legal basis for recording this information is, and make sure customers understand what data will be used and why. Communications should be appropriate, taking into account customers' needs and abilities.

Organisations will also need to carefully consider how they ensure compliance with all the data protection principles – including those relating to appropriate grounds for processing, data minimisation, accuracy, security and retention - whilst meeting their obligations under Ofgem's principles.

Questions 13: Do you support our proposal to extend the requirement to keep records for two years to include telephone sales and marketing? If not, please explain why, including the scope of any increase in costs.

Question 14: Do you agree with our rationale for not applying the requirement to keep records to include online sales? What would be the implications of extending the requirement to online sales (eg impact on PCWs, increased costs)?

These questions relate to the retention of records which will include personal data. Data protection requirements dictate that personal data should be retained for no longer than is necessary. It is for organisations to determine what is necessary, but a regulatory requirement to retain a record, or class of records, would be a relevant factor. It is unclear why two years has been deemed to be the appropriate time period in this case though. Organisations must also continue to have a relevant legal basis to continue to process and retain the data.