The Information Commissioner's response to the Ofcom consultation on the general conditions relating to consumer protection

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 updating the regulatory rules applying to communications providers (CPs) in relation to consumer protection matters.

The Commissioner's response to this discussion paper 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 Ofcom with further advice or assistance on the data protection implications of these proposals, if needed.

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 - as Ofcom will be aware - this may lead to changes to PECR. We would be happy to provide further advice and guidance on the potential impact of these reforms. Links to guidance on the GDPR and its requirements is available on the Information Commissioner's Office website, www.ico.org.uk.

Question 1: Do you agree with our overall approach to this review of the general conditions as set out in sections 2 and 3 of this consultation? Please give reasons for your views.

Yes. Updating the general conditions to take into account any changes in consumer behaviour and developments in technology appears to be a sensible way to ensure the conditions remain relevant and effective. In complying with the general conditions, organisations will also need to take account of their legal obligations under data protection law. It is important that regulatory rules arising from different regulatory areas do not create conflicting requirements. The Information Commissioner is committed to working with Ofcom to help address any potential conflicts that may arise.

CPs may hold and use information about both users and subscribers. It is important for providers to ensure any personal data they collect and use is handled in a way that meets data protection requirements.

The Commissioner agrees that vulnerable people should be treated fairly and that CPs should accommodate their needs. A more detailed description of what 'vulnerability' means in the context of the general conditions may be helpful. In the broadest sense, our understanding is that vulnerability may be a permanent or temporary state and may arise from a wide variety of circumstances.

Data about some of the conditions under which individuals may be considered vulnerable - such as those relating to their physical and mental health - will constitute 'sensitive personal data' under the DPA; under the GDPR this is deemed 'special category' personal data. Data protection law provides extra protections with regards to sensitive/special category data. It is important that CPs understand whether the data they are collecting and using in order to meet the conditions of entitlement constitutes sensitive/special category personal data. In particular, CPs will need to carefully consider their legal basis for collecting and using sensitive/special category personal data.

CPs should also be careful to only collect the minimum amount of information necessary to meet individuals' needs. Commonly this may take the form of recording a 'needs code'. CPs will also need to communicate clearly to individuals the purposes their data will be used for and why. They should carefully consider how best to communicate with vulnerable consumers, taking account of individual needs and abilities.

If CPs seek to rely upon explicit consent as a means to process sensitive/special category personal data then they must ensure this meets the high standard set out under the GDPR. The ICO is currently consulting on guidance concerning consent requirements under GDPR.

Question 2: Do you agree with our proposed implementation period for the revised general conditions of 3 to 6 months following publication of our final statement? If you think a longer

implementation period is necessary, please explain why, giving reasons for your views.

It is for Ofcom to determine the appropriate implementation period. As the GDPR will apply from 25 May 2018, CPs should take account of the changes to data protection law when implementing changes to reflect the revised general conditions.

Question 7: Are there any other modifications to the conditions relating to information publication and transparency requirements that you consider would be appropriate?

Data protection law places organisations under a duty to ensure individuals are given clear information about how their personal data will be collected and used. This is set out in the ICO code of practice on privacy notices and aligns with the transparency requirements proposed by Ofcom.

Question 14: Do you agree with our proposals to introduce a new requirement for communications providers to take account of, and have procedures to meet, the needs of consumers whose circumstances may make them vulnerable?

Yes. The Commissioner agrees that the needs of vulnerable people should be taken into account by CPs. Introducing the new requirement may be an effective way to address this.

As outlined above, clarifying the meaning of 'vulnerable' will be important. CPs will need to be clear about how they intend to collect information to identify vulnerable consumers, and will need to communicate that to consumers. CPs should determine what their legal basis for collecting and using that information will be before starting to process it.

When information about vulnerability is recorded, CPs should take care to ensure they are clear about how and why that data will be processed. People may be considered vulnerable for a wide range of reasons, which may include difficulties in using some types of communication. CPs will need to consider how to effectively communicate with individuals with a variety of needs.

Irrespective of whether the data falls within the definition of sensitive/special category personal data, there may be significant detriment to individuals if information is disclosed inappropriately or mishandled. CPs should take care to only collect the information necessary for the purposes they need it, and ensure robust procedures are in place for handling the data appropriately.

The Information Commissioner recommends the use of Privacy Impact Assessments (PIA). A PIA will help to identify the privacy and data protection risks arising, and the steps that may be taken to address or mitigate those risks. The Information Commissioner has published a Privacy Impact Assessments Code of Practice.

Question 15: Do you agree with our proposals to update regulation by extending the current protections for end-users with disabilities, which currently apply only in relation to telephony services, to cover all public electronic communications services?

There are advantages to extending the protections, but the Commissioner is not in a position to determine whether extending the protections will be an appropriate step. She is mindful that personal data should be used in a way that complies with data protection requirements.

The data protection principles require that personal data should be used fairly, and that it should not be used for purposes which are incompatible with those for which it was originally collected. If CPs intend to use existing data on individuals with disabilities more widely, then they will need to inform them about what they intend to do and why. The Commissioner strongly recommends undertaking a PIA in order that privacy and data protection risks may be identified and appropriate steps put in place.

It will also be necessary to make sure that the data collected is not excessive. In this context, it may be more appropriate to record information about a person's needs, rather than details of their condition or vulnerability.

Question 18: Do you agree with the changes we are proposing to make in relation to the provision of calling line identification facilities, including the new requirements we are proposing to add? Please give reasons for your views.

The Commissioner appreciates the intrusive, disruptive and upsetting effect that nuisance calls can have on individuals. The Commissioner is supportive of the measures set out in the consultation to require all CPs to be satisfied that full caller line identity (CLI) information is present in telephone calls in transit through the telephone system.

While this will likely help to reduce the number of calls with incomplete CLI information, it does not appear to address situations where valid, but false, CLI credentials are presented. The ICO sometimes receives information from individuals or organisations whose CLI information has been falsely presented by nuisance callers.

The Commissioner welcomes the recognition that Regulation 10 of PECR requires that callers have a simple means of withholding their line information from the call recipient. This is balanced by Regulation 11 of PECR that requires that individuals must have a free means by which to automatically reject calls where CLI has been withheld from them.

We understand that the CLI information should remain available to the telecommunications services through which a call is routed.

Question 20: Do you agree with our proposal to remove the current provision which expressly prohibits so-called 'reactive save' activity (in GC 22.15)?

Altering the 'reactive save' prohibition would need very careful consideration.

In the proposed changes to 'reactive save' activities, individuals would be marketed to. Both the DPA and PECR regulate marketing activity in different ways. Whether a reactive save will be appropriate will depend on whether an individual has consented to marketing, and when consent was gained. The ICO's Direct Marketing Guidance provides relevant advice in paragraphs 102 and 194:

102: If a customer gives consent when signing up to a service, consent is likely to expire if they subsequently cancel their subscription. The organisation should not rely on that consent to send further unsolicited messages to win the customer back.

194: However, we recognise that people can change their minds and that marketing strategies also change. There is some merit in making sure that the information about people's preferences is accurate and up to date. We consider that it can be acceptable to send a message immediately after someone has opted out confirming they have unsubscribed and providing information about how to resubscribe, or to remind individuals that they can opt back in to marketing if the reminder forms a minor and incidental addition to a message being sent anyway for another purpose. However, organisations must do this sensitively, must not include marketing material in the message, and must never require an individual to take action to confirm their opt-out.

If an individual has issued a notice in writing that they do not wish to receive marketing, this will constitute a section 11 request under the DPA. Organisations should honour section 11 requests they receive, irrespective of other circumstances.

PECR regulates marketing communications sent by electronic means, including telephone calls, emails and text messages, but not postal

communications. Losing providers that want to market to their customers should consider the whether they can meet the obligations placed on them by Regulations 19-23 of PECR prior to sending marketing communications by electronic means.

Revisions to the ePrivacy Directive are currently being negotiated in Europe and may also affect marketing practices. CPs should consider the impact of the ePrivacy Regulation once this has been agreed.

Question 21: Do you agree with our proposal to replace the current mis-selling provisions with rules that focus on the information that communications providers give to customers when selling or marketing fixed-line or mobile communications services? Please give reasons for your views.

While the mis-selling provisions are mainly concerned with the provision of accurate information, communications promoting products and services will fall under the definition of marketing. The instigation and transmission of marketing must comply with the DPA and PECR, as set out in the response to Question 20.

Section 12.11 of the consultation is concerned with keeping separate records of individuals' consent to switch provider. This aligns with the GDPR requirements regarding consent for processing personal data, which require that consent is unambiguous, requires a positive action to be undertaken, and is recorded.

The Commissioner notes that section 12.30 (b) proposes that CPs undertake due diligence checks on the directors of retailers. As this would entail processing the directors' personal data, CPs will need to ensure that those directors are aware that their personal data will be collected and used in this way. Individual directors should be aware that any periods of disqualification will be checked, and what the purpose in checking that information will be.