The Information Commissioner's Office response to the statement and consultation on the processes for switching fixed voice and broadband providers on the Openreach copper network

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). He 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 he can, and taking appropriate action where the law is broken.

The Information Commissioner welcomes the opportunity to respond to this statement and consultation on the processes for switching fixed voice and broadband providers on the Openreach copper network.

In this response we have focussed only on those issues which impact on information rights.

Question 1
Q1: Do you agree with our assessment of the Record of Consent Requirement?

Question 1 - Response:
We understand you have considered the impact of this new requirement on both consumers and providers and that the main reasons for this requirement are to protect consumers against slamming, as well as to assist Ofcom in enforcement action against such activities. We agree with the overall approach of obtaining customer consent to switch and the requirement to keep a record of this consent.

The first data protection principle states that personal data should be processed fairly and lawfully and requires that there is at least one legitimate basis for processing. One such basis is that the individual has given their consent to the processing of their personal data, although

there are a number of other conditions within the DPA that are equally valid.

Consent is not defined by the DPA. However, the European Data Protection Directive (95/46/EC) defines consent as:

"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

The definition states an individual must "signify" their agreement; this means that there must be some active communication between parties. An individual may however "signify" their agreement by means other than writing.

We note the options set out in 9.23 that are considered to constitute a record of consent: a call recording, a written record or, for online communications, screen shots of order systems and account interactions. These stated methods of obtaining consent would not conflict with the requirements of the DPA providing that consent has been obtained in compliance with the definition above.

Irrespective of the format the consent takes, or how it is recorded, the most important point when obtaining consent is that it is clear to individuals what they are consenting to, and the individual should be fully aware of what they are consenting to and how their data will be processed.

We note the consultation discusses the means by which consent can be collected (section 9.23) and what the 'record of consent' should contain (section 9.24), however the consultation does not discuss requirements for what will be communicated to individuals in obtaining their consent. Looking to the definition above, the information given to individuals is vital to ensure that any consent obtained is appropriately informed. It may also be worth noting that consent obtained under duress or on the basis of misleading information would not adequately satisfy the requirements of the DPA. The following link to our website discusses consent in more detail:
http://www.ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing.

We understand that the proposal is to keep the 'record of consent' for 12 months. We understand Ofcom have pointed out why they believe 12 months is necessary in section 9.36, including where there may be a delay in the individual reporting the incident, for monitoring purposes and where evidence may come to light over a longer period. The DPA does not set specific time limits for retaining personal data, however consideration

should be given to the fifth principle, which states that personal data kept for any purpose shall not be kept longer than is necessary for that purpose and the third principle which states personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Provided this retention period is based on sensible and justifiable reasoning that it is necessary to retain the record of consent for 12 months, it is likely to be compliant with the DPA.

Question 2
Q 2: Do you agree with our assessment of the requirement for better information on the implications of switching?

Question 2 - Response:
Our understanding of this is that it is proposed the losing provider (the LP) is required to provide better information in the notification of transfer letter sent to the consumer on the implications of switching.

We agree with an approach where consumers are given better information as we have always encouraged transparency in the handling of personal data. In particular the first principle of the DPA requires that the processing of personal data must be fair and lawful. Fairness generally requires that an organisation is transparent, open and clear with individuals. If individuals have not been given adequate information to enable them to understand how their collected personal data will actually be used, then that collection of data will be unfair and not compliant with the DPA in its own right. Advice on conveying information to individuals in an accessible way can be found in our Code of Practice on providing privacy notices: Privacy Notices Code of Practice.

Question 4
Q4: Do you agree with our assessment of requirements to reduce the occurrence of ETs under the WLT process?

Question 4 – Response
The seventh principle of the DPA states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. We would therefore agree with an approach where additional measures are taken to protect against occurrences where unauthorised processing of personal data could occur.

We would note, however, that whilst the requirement that no working line takeover (WLT) order is placed without an exact match and the requirement for the LP to notify end users under the WLT process may act

to reduce the occurrences of Erroneous Transfers (ETs), this may not address other underlying issues with the data which is being relied upon. There is an obligation on organisations to ensure that the personal data they hold and use is accurate and up to date (the fourth principle). If errors are frequently occurring in the underlying data, it may be that practices need to be reviewed.

Question 6
Q6: Are there any other key issues that need to be taken into consideration?

Question 6 - Response:
We understand that other DPA concerns, mainly data security concerns, are specifically addressed at section 8.59, however this appears to relate to the use of a database. Having digested other sections of the consultation, namely sections 8.95 and 8.96, it does not appear the use of a database is a proposal Ofcom are taking forward at this stage. However should Ofcom decide to take this option forward in the future we would be happy to assist with any data protection queries Ofcom may have in the implementation a database.

October 2013