The Information Commissioner's response to the Competition and Markets Authority's consultation: "Consumer law compliance review: cloud storage"

1. Introduction

The Information Commissioner is responsible 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.

We welcome the opportunity to respond to the CMA's consumer law compliance review of cloud storage. The observations we wish to make regarding cloud storage services do not directly address the specific questions set out in the consultation response form, but we feel these are relevant and therefore we've set out our comments below.

2. Cloud services and the DPA

The Information Commissioner recognises the benefits that cloud storage services offer to consumers and businesses, such as the ability to backup data to protect it from loss, and the ability to easily access the information stored from multiple devices.

It is important to note that cloud providers may be data controllers for the purposes of the DPA, and they must comply with data protection principles when processing personal data (see annex).

We have published guidance for organisations on the use of cloud computing.[1]

The nature of cloud computing is such that consumers may be contracting with cloud services based solely outside the territorial scope of UK domestic data protection law, or its European equivalents. It can

[1] https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

sometimes be difficult to know exactly where data stored "in the cloud" is actually held and processed. Data may be being held in another country, and sometimes copies of the data will be held in multiple countries. This may create uncertainty, as well as practical difficulties, for individuals when they seek to exercise or enforce their legal rights.

3. Giving consumers information and control

The first principle of the DPA requires that personal data is processed fairly. An essential element of fairness is ensuring individuals are given sufficient information to understand how their personal data is being processed. In data protection terms this is commonly referred to as giving fair processing information. In practice this means that cloud storage providers should make clear, in ways that individuals can easily understand, the terms and conditions under which the cloud service is provided, and any other information needed to make the processing in question fair.

The provision of clear information is particularly important when a service provider is further processing data in ways that extend beyond simple file storage, for example if content is to be scanned by the provider for the purpose of targeted advertising. Any such processing must comply with the data protection principles and be clearly explained so that choice and control may be genuinely exercised by consumers in an informed way.

In some cases individuals may not even be aware they are using a cloud storage service. A number of devices, such as smartphones, tablets and personal computers, now include cloud storage services as an integral part of their operating system, or it comes pre-installed on a device. Such services may be turned on by default, and so well integrated that it can be difficult to tell what data is being held locally on the device and what is stored remotely. It is therefore important that manufacturers present choices in a clear manner and give consumers sufficient control over the processing of their data.

It's important that individuals retain the ability to manage their data once they have uploaded it to a cloud storage service. For example, if an individual chooses to delete their data, then it should be deleted by the service provider and not retained. Consumers should also be able to exercise control by being able to quickly and easily move their data from one service to another if they so wish. It should be noted that data portability will become a specific right in relation to information society

services under the recently agreed General Data Protection Regulation (GDPR).[2]

4. Security of the data

It is vital that cloud storage services are kept secure, and that data is adequately protected from accidental loss, unauthorised access or theft. Individuals may store very sensitive information with storage providers and disclosure could cause them significant damage or distress.

Principle 7 of the DPA requires data controllers to take appropriate technical and organisational measures to protect the security and integrity of the personal data they process (see annex). Cloud providers should therefore take all reasonable steps to ensure that the data they are storing is secure.

The Information Commissioner is happy to provide any further advice and assistance the CMA may require concerning the data protection obligations and privacy aspects of cloud computing services.

January 2016

[2] http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Annex – Principles of the Data Protection Act 1998

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

    (a) at least one of the conditions in Schedule 2 is met, and

    (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. 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

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.