Data Protection Act 1998

Guidance on the use of cloud computing

ico.

Information Commissioner's Office

Contents

1. The Data Protection Act 1998 (DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

2. An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

3. This is part of a series of guidance that goes into more detail than the Guide, to help organisations to fully understand their obligations as well as promote good practice.

4. This guidance explains what you should consider prior to a move to cloud computing for the processing of personal data.

Overview

- Cloud computing services offer organisations access to a range of technologies and service models typically delivered over the internet.

- Organisations that maintain and manage their own computer infrastructure may be considering a move to cloud computing to take advantage of a range of benefits that may be achieved such as increased security, reliability and resilience for a potentially lower cost.

- By processing data in the cloud an organisation may encounter risks to data protection that they were previously unaware of. It is important that data controllers take time to understand the data protection risks that cloud computing presents.

- This guidance offers a set of questions and approaches an organisation should consider, in conjunction with a prospective cloud provider, in order to ensure that the processing of personal data done in the cloud complies with the DPA.

Introduction

5. A shift towards a greater use of cloud computing is well underway. Innovative products, mobile access to data and affordable pricing structures are often cited as key drivers for an organisation to consider a move to cloud computing. Cloud services also offer an affordable route for smaller organisations

(including start-up companies) to cope with rapid expansion. The UK government's commitment to adopt greater use of cloud services is demonstrated in the G-Cloud programme which has put together a catalogue of cloud information and communications services available to the UK public sector.

6. The ICO published the Personal information online code of practice in July 2010. The code explains how the DPA applies to the collection and use of personal data online. It provides practical advice for organisations that do business or provide services online.

7. The Personal information online code of practice briefly discussed the use of cloud computing in relation to processing personal data online. Given the increased usage of this technology the ICO has decided to provide a more comprehensive explanation of the data protection compliance issues that can arise when personal data is processed in the cloud.

8. This guidance is aimed primarily at organisations using cloud services or considering a move to cloud services – it tells them what they need to take into account.

9. Cloud providers should use this guidance so that they are aware of the data protection issues that their current and prospective cloud customers may need to deal with. This could help cloud providers to make their services more attractive to customers that are subject to data protection law.

What is cloud computing?

10. Cloud computing is a term used to describe a wide range of technologies, so it is important to be clear about what we mean by cloud computing in this guidance.

11. We use a broad definition of the term in this guidance in order to cover all the main implementations of cloud computing.

Definitions

12. Cloud computing is defined as access to computing resources, on demand, via a network.

13. In more detail this covers:

- **computing resources –** this can include storage, processing and software;

- **on demand –** the resources are available on a scalable and elastic basis. This typically involves the dynamic provision of virtualised resources. Users are often billed for the level of resource used; and

- **via a network –** the transit of data to and from the cloud provider. The transit of data may be over a local or private network or across the internet.

14. For further clarity we have defined the three main groups involved in the use and delivery of cloud services.

- **Cloud provider** – The organisation that owns and operates a cloud service (Note: More than one cloud provider may be involved in the supply chain of a single cloud service).

- **Cloud customer** – The organisation that commissions a cloud service for a particular purpose.

- **Cloud user** – The end user of a cloud service – for example a member of the public.

Deployment models

15. Cloud computing can be deployed using a number of different models.

- **Private cloud** – The cloud customer is the sole user of the cloud service. The underlying hardware may be managed and maintained by a cloud provider under an outsourcing contract. Access to the cloud service may be restricted to a local or wide area network.

- **Community cloud** – A group of cloud customers access the resources of the same cloud service. Typically the cloud customers will share specific requirements such as a need for legal compliance or high security which the cloud service provides. Access to the cloud service may be restricted to a wide area network.

- **Public cloud** – The infrastructure, platform or software is managed by the cloud provider and made available to the general public (cloud customers or cloud end-users). Access to the cloud service is likely to be over the public internet.

- **Hybrid cloud** – Describes a combination of private, community and public clouds. A cloud customer will segregate data and services across different cloud services, with access between them restricted depending on the type of data they contain.

Service models

16. Although the term cloud computing may be applied to a range of technologies there are three main types of cloud service.

- **Infrastructure as a Service (IaaS)** – An IaaS cloud offers access to the raw computing resources of a cloud service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud provider's hardware according to the capacity required.

> **Example**
> A software development company is building an application for a client. It needs to test the application before transferring it to the live environment. By using an IaaS cloud service it can simulate an environment which is identical to the live server (except that dummy data will be used) without the need to purchase additional hardware during this relatively short phase of the development process.
>
> At the end of the testing process all the data will be deleted from the cloud service and the application delivered to the client.

- **Platform as a Service (PaaS)** – A PaaS cloud offers access to a computing platform which allows cloud customers to write applications to run within that platform, or another instance of it. The platform may in turn be hosted on a cloud IaaS.

> **Example**
> A social networking service offers a platform which allows software developers to create third party applications which takes advantage of the existing functionality of the social network – for example functions to access user data or the ability to post messages to other users. The products developed by third parties will only operate within the confines of the social network platform.

- **Software as a Service (SaaS)** – A SaaS cloud offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure.

Example
A start-up company is expanding rapidly and wants to use customer relationship management (CRM) software to keep track of its customers and sales. It identifies a cloud provider offering CRM software, accessed through a web browser, as being appropriate for its needs.

Each employee within the company is given a username and password to access the software to enter new data or to access existing data. The software can be accessed by employees whilst working away from the office.

Layered services

17. As explained in the description of service models above, one cloud service can be layered on top of another. The cloud provider offering one part of the cloud service, eg the software, may not be the same as the provider operating another component, eg the cloud platform or infrastructure.

18. These layered services can result in a more complex supply chain of cloud providers.

Example
Company A provides calendar and scheduling software hosted in the public cloud. The software allows cloud users to schedule appointments and access the appointments of other users (where they are authorised to do so).

The cloud software is owned by Company A and offered as a cloud computing SaaS product.

Company A hosts its software on an IaaS cloud which is owned and operated by Company B.

How does the Data Protection Act apply to information processed in the cloud?

19. The DPA applies to personal data that is processed. Processing has a very broad definition and is likely to include most of the operations that are likely to occur in the cloud, including simply storage of data.

20. The DPA defines personal data as "data which relate to a living individual who can be identified from that data or from that data and other information which is in the possession of, or likely to be in the possession of, the data controller." For more information on what constitutes personal data see the ICO's guidance on Determining what is personal data.

21. If you are currently a data controller, this will continue to be the case if you move that processing to the cloud.

Identify the data controller

22. The data controller has ultimate responsibility for complying with the DPA. The use of layered services mean that it is possible that a number of data controllers, and data processors working on their behalf, could be acting together to deliver content or services which involve the processing of personal data in the cloud.

23. In cloud computing it will be the cloud customer who will determine the purposes for which and the manner in which any personal data are being processed. Therefore it is the cloud customer who will most likely be the data controller and therefore will have overall responsibility for complying with the DPA.

24. The precise role of the cloud provider will have to be reviewed in each case, in order to assess whether or not it is processing personal data. If it is, it is important to determine whether the cloud provider is merely acting as a 'data processor' on behalf of the data controller or whether it is a data controller in its own right.

25. The ICO has previously published guidance on Identifying data controllers and data processors.

Data controller in a private cloud

26. Identifying the data controller in a private cloud should be quite straightforward because the cloud customer will exercise

control over the purpose for which the personal data will be processed within the cloud service.

27. If a cloud provider is contracted simply to maintain any underlying infrastructure then it is likely to be a data processor, ie it will only process the data on behalf of the data controller. This will include tasks such as allocating computing resources, performing and storing back-ups, providing support.

Data controller in a community cloud

28. In a community cloud more than one data controller is likely to access the cloud service. They could act independently of each other or could work together, for example where they are involved in a joint enterprise.

29. If one of the data controllers also maintains the cloud infrastructure, ie it is acting as a cloud provider, it will now also assume the role of a data processor in respect of the various data controllers that use the infrastructure.

30. If the cloud customers intend to share data between themselves they must take the time to clarify their roles and be clear as to the extent to which they will be acting as data controllers in relation to the shared data. When sharing personal data cloud customers should also consider the ICO's Data sharing code of practice.

Data controller in a public cloud

31. When using a public cloud, the ICO recognises that a cloud customer may find it difficult to exercise any meaningful control over the way a large (and perhaps global) cloud provider operates. However, simply because an organisation chooses to contract for cloud computing services on the basis of the cloud provider's standard terms and conditions, does not mean that the organisation is no longer responsible for determining the purposes for which and manner in which the personal data is to be processed. The organisation will continue to be a data controller and will be required to meet its obligations under the DPA.

32. There are a wide range of cloud services available which should enable the cloud customer to choose a cloud service which best suits its specific needs – including its need to comply with the DPA. The cloud customer does not transfer data protection obligations to the cloud provider simply by choosing to use its services in order to process his personal data.

33. If a cloud provider plays a role in determining the purposes for which the personal data are processed, ie it uses the personal data for its own purposes, then it will also be a data controller and will take on its own data protection responsibilities.

Example
An organisation wishes to expand its online presence to include social media. The organisation develops a third party application to run within a social network platform.

The organisation will be a data controller for any personal data it processes through users choosing to use its application, integrated with the social network or for any other data collected through usage of the application.

The social network platform will be acting as a data controller for any personal data processed by the social network. This may also include processing done for advertising or marketing purposes.

Where the personal data is being used by both organisations for their own purposes, they will both be data controllers.

Responsibilities of the data controller

34. In addition to the responsibilities relating to collection, storage and retention of personal data outlined in the Personal information online code of practice, the use of cloud computing may introduce a set of compliance requirements which a data controller may not have encountered previously.

35. Cloud computing is not a one-size-fits-all product and in many cases it can be tailored to fit the specific needs of an organisation. The compliance issues that arise will depend on the type of cloud service in question.

36. Any organisation considering a move to the cloud must have a clear understanding of its needs and obligations in order to ensure that it uses an appropriate cloud provider.

Select which data to move to the cloud

37. It is important to remember that a cloud customer may not need to move all its data into the cloud or into the same cloud service.

38. The processing of certain types of personal data could have a greater impact on individuals' privacy than the processing of others. With this in mind, the cloud customer should review the personal data it processes and determine whether there is any data that should not be put into the cloud. This may be because specific assurances were given when the personal data was collected. Often, the question may not be whether the personal data should be put into the cloud but what the data protection risks are and whether those risks can be mitigated.

39. The cloud customer should create a clear record about the categories of data it intends to move to the cloud. This could be data for certain types of customer or data relating to certain types of transaction.

40. The cloud customer should also bear in mind that using cloud services may give rise to more personal data being collected. For example, the usage statistics or transaction histories of users may start to be recorded. This 'metadata' may also be personal data in certain circumstances. If so, the cloud customer must ensure that it knows what is being collected, determine whether this is necessary and make sure that cloud users are provided with sufficient information about this, for example through a privacy policy.

Assess the risks

41. Before considering which cloud service or cloud provider is right for an organisation the cloud customer must also consider how it intends to process personal data in the cloud.

42. Once the cloud customer is clear which personal data it holds and how it intends to process it in the cloud, it can then assess the risks and take appropriate steps to mitigate them.

Example
A school is considering expanding its computer facilities by converting two classrooms to computer rooms. Traditionally this would require the appropriate software licences for each computer. If it switches to a cloud-based SaaS model for some software it expects to have lower overall licensing and maintenance costs.

An online productivity suite would allow students remote access to their work and other educational resources. If personal data such as student assessment, attainment or attendance data were transferred to the cloud service they may not be adequately

protected, eg against unauthorised access if the cloud service does not have proper authentication controls.

The school determines that the cloud service must only be used for student work and educational resources and retains the existing network for staff to process personal data of the students.

43. Cloud customers who are looking to process personal data in large or complex cloud services would benefit from conducting a privacy impact assessment in order to assess and identify any privacy concerns and address them at an early stage.

Select the right cloud service and cloud provider

44. A wide range of cloud services exist to achieve various goals. It may be appropriate to use a cloud service which was designed for the specific processing rather than one which could be adapted, as there is a risk that customisation may introduce an additional set of risks.

45. Different cloud providers and cloud services have reached different stages in the development and maturity of their services and may target particular market sectors. For example, some cloud services are aimed at consumers whereas others are bespoke tools built for particular niche organisations.

Monitoring performance

46. The obligations of the cloud customer as a data controller will not end once a cloud provider is chosen. A continual cycle of monitoring, review and assessment are required to ensure that the cloud service is running in the manner expected and as the contractual agreement stipulates.

47. In the case of layered services, the cloud provider must keep the cloud customer informed of changes in the chain of sub-processors that take place during the course of providing the cloud service.

Informing cloud users

48. The cloud customer may need to take appropriate steps to inform the end users of the cloud service about the processing arrangements that the controller has put in place. As a matter of good practice, cloud customers should be as open as possible about this.

Get a written contract

49. The DPA requires the data controller to have a written contract (Schedule 1 Part II paragraph 12(a)(ii)) with the data processor requiring that the "data processor is to act only on instructions from the data controller" and "the data processor will comply with security obligations equivalent to those imposed on the data controller itself."

50. The existence of a written contract should mean that the cloud provider will not be able to change the terms of data processing operations during the lifetime of the contract without the cloud customer's knowledge and agreement.

51. Cloud customers should take care if a cloud provider offers a 'take it or leave it' set of terms and conditions without the opportunity for negotiation. Such contracts may not allow the cloud customer to retain sufficient control over the data in order to fulfil their data protection obligations. Cloud customers must therefore check the terms of service a cloud provider may offer to ensure that they adequately address the risks discussed in this guidance.

Example

An organisation wanted to add a forum to its website to allow customers to interact and give feedback on its products and services. The organisation identified a SaaS cloud provider that could offer this solution.

As the data controller, the cloud customer stipulated that the cloud provider must not use the personal data of the forum users for its own purposes, for example, by using their email address for third party advertising.

At a later date, the cloud provider tried to update the terms and conditions in an attempt to allow it to change the conditions of processing and to use the data for its own purposes.

The existence of a written contract between the cloud customer and cloud provider meant that this change of processing could not take place without the cloud customer's agreement and consequently the personal data was protected from any further processing which would be contrary to the terms of the data processing agreement.

Selecting a cloud provider

52. An important part of selecting the right cloud provider will be an assessment of the security that the cloud provider has in place. It is important to remember that security is not the only factor that must be considered, but it is a very important one.

53. This section sets out the issues the cloud customer should consider and the questions the cloud customer should ask a cloud provider, if they have not provided this information already.

Assessing the security of a cloud provider

54. The DPA requires that data controllers take "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

55. When processing is undertaken by a data processor, the data controller must choose a processor providing sufficient guarantees about the technical and organisational security measures governing the processing to be carried out, and must take reasonable steps to ensure compliance with those measures.

56. The cloud customer should therefore review the guarantees of availability, confidentiality and integrity that the cloud provider provides.

57. Usually one of the most effective ways to assess the security measures used by a data processor would be to inspect their premises. The ICO recognises that, particularly in the case of the public cloud, this is unlikely to be practicable for various logistical reasons. It is also unlikely that a cloud provider would be willing to permit each of its prospective and current customers to enter its premises to carry out an audit.

58. One way for cloud providers to deal with this problem would be for them to arrange for an independent third party to conduct a detailed security audit of its service and to provide a copy of the assessment to prospective cloud customers. The assessment should be sufficiently detailed to allow the cloud customers to be able to make an informed choice as to whether the provider's security is appropriate and will, in turn, help the cloud customer to comply with its data protection obligations.

59. The assessment should include the physical, technical and organisational security measures in place and be appropriate for the particular cloud service.

60. In the case of layered cloud services, this assessment should include appropriate assurances that the security of each sub-processor likely to be involved in the processing of cloud customer's data will comply with security requirements set out by the cloud provider.

61. The cloud provider should also be able to provide the cloud customer with regular updates showing that appropriate security measures continue to be in place (and are kept up to date where necessary).

62. To assist cloud customers in assessing the security offered by a cloud provider, the ICO supports the use of an industry recognised standard or kitemark. Such a scheme would help cloud customers to compare the services offered by cloud providers and be confident that any independent assessment of the cloud service was sufficiently thorough. However, cloud customers still need to comply with the DPA even if their cloud service provider has a particular kitemark – a kitemark is unlikely to address all aspects of data protection compliance.

Protecting your data

63. Encryption allows a cloud customer to ensure that the personal data they are responsible for can only be accessed by authorised parties who have the correct 'key'.

64. Data 'in transit' between endpoints should be secure and protected from interception. This can be achieved by using an encrypted protocol. The encryption algorithm used should meet recognised industry standards.

65. The cloud provider should also be able to give assurances that data in transit within the cloud service is appropriately secure. This includes data transferred between data centres which may be separated geographically.

66. The cloud customer should also consider if it is appropriate to use encryption on data 'at rest', ie when stored within the cloud service. This will depend on the nature of the personal data and the type of processing being undertaken in the cloud. This will be an important consideration when sensitive personal data is being processed.

67. In an IaaS or data storage scenario, it is much easier for the cloud customer to insist that all data is encrypted before it leaves his, or the cloud user's device. However, in a SaaS cloud this is more difficult to achieve because the cloud provider may need access to the data in order to perform the necessary processing.

68. If encryption is used as a technical measure to secure data, it is important to ensure the security of the key. A robust key management arrangement is crucial to maintain the level of protection encryption can offer.

69. It is also important to note that the loss of an encryption key could render the data useless. This could amount to the accidental destruction of personal data – this would be a breach of the DPA's security principle.

Example
An organisation performs weekly manual back-ups. These are stored on external drives. The drives are stored in a locked cabinet when not in use.

Moving to a cloud-based backup solution has a number of benefits including:

- automating the process;
- the ability to run nightly back-ups;
- storing back-ups off-site; and
- reduced risk of theft.

The organisation opts for a cloud-based backup solution which encrypts files before transmitting them over a secure connection to the cloud provider. The key is kept in the secure possession of the cloud customer.

The cloud provider is therefore unable to view or otherwise further process the data other than to maintain access to, and availability of, the data.

The organisation may test the back-up service regularly by attempting to restore files held in the cloud.

Access control

70. One of the benefits of using a cloud service is the ability to access the data from any location. This means that cloud users can access the same data from the office or home and from a range of different devices. However, the cloud customer must

ensure there are sufficient measures in place to prevent unauthorised access to the data.

71. If a cloud service offers an authentication process, for example, using a username and password system, cloud users must each have their own accounts.

72. There should also be a system in place to create, update, suspend and delete user accounts, to remove access from employees when they leave the organisation or to reset forgotten, lost or stolen credentials.

Example
An organisation has implemented a cloud-based email service for its employees. Employees can access this account from the office, from personal computers at home and through mobile devices such as smartphones and tablets.

An employee accessed the email service from a personal computer at home. The PC had no security protection in place and was infected with key-logging malware. The employee's username and password were captured and transmitted to the malware author who was then able to gain unauthorised access to the email account, the contents of which contained personal data of the organisation's clients.

This breach of personal data occurred because the data controller did not ensure that the IT its employees used to access its system was adequately protected.

Data retention and deletion

73. When data is deleted is it rarely removed entirely from the underlying storage media unless some additional steps are taken. In addition, a cloud provider is likely to have multiple copies of data stored in multiple locations to provide a more reliable service. This may include back-up tapes or other media not directly connected to the cloud. Copies of personal data stored in a cloud service may also be stored in other forms such as index structures.

74. The cloud customer must ensure that the cloud provider can delete all copies of personal data within a timescale that is in line with their own deletion schedule.

75. The cloud customer should find out what will happen to personal data if it decides to withdraw from the cloud service in the future.

Provider access

76. If the cloud provider is managing the computing resources on behalf of the cloud customer it is likely that it will be able to access copies of the data. Access may be authorised for actions such as the provision of support services. However, unauthorised access may lead to the inappropriate disclosure, deletion or modification of personal data.

77. There should be a clear policy in place to specify the circumstances in which the cloud provider may access the personal data it processes. The policy should provide for an audit process that will alert the cloud customer if unauthorised access, deletion or modification occurs.

Further processing

78. The second data protection principle states that "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."

79. The cloud customer should ensure that the cloud provider only processes personal data for the specified purposes. Processing for any additional purposes could breach the second data protection principle. This might be the case if the cloud provider decides to use the data for its own purposes. Contractual arrangements should prevent this.

80. A number of SaaS products are supported by advertising that is based on the personal data of cloud users. In order to target advertisements the cloud provider will need access to the personal data of the cloud users. A cloud provider may not process the personal data it processes for its own advertising purposes unless this has been authorised by the cloud customer and the cloud customer has explained this processing to cloud users. Remember that individuals have a right to prevent their personal data being used for the purpose of direct marketing.

81. The cloud provider must not process the cloud customer's or cloud user's personal data without the agreement of the cloud customer.

Using cloud services from outside the UK

82. The computing resources managed by a cloud provider may be located outside the UK. A large cloud provider may have a number of data centres, each of which could be located in a different country. This distributed architecture can improve reliability of the cloud service but also means that it can be difficult to know where data is being processed.

83. The DPA requires that personal data "shall not be transferred to any country or territory outside the European Economic Area (EEA) 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."

84. Cloud customers should ask a potential cloud provider for a list of countries where data is likely to be processed and for information relating to the safeguards in place there. The cloud provider should be able to explain when data will be transferred to these locations.

85. In the case of layered cloud services, information relating to the location of each sub-processor involved in the processing of the data should also be available from the cloud provider, with details of the security arrangements in place.

86. The ICO has already prepared detailed guidance on how to determine the adequacy of protection in relation to international transfers of data.

Example
An IaaS cloud provider informs a potential cloud customer that it operates six data centres globally: two in the EEA; two in North America; and two in Asia.

It also has a support centre which is located in the USA.

The cloud provider can guarantee that all personal data will be stored in the geographical area that the potential cloud customer specifies. The potential customer specifies that their data must only be stored within the EEA.

However, during a support call personal data may be transferred to the USA. The cloud provider must make the potential customer aware that its guarantee to store data only within the EEA does not include transfers of data to the USA for support services. This will allow the potential customer to make an informed decision about whether it wishes to use this particular cloud provider.

Example
An IaaS cloud provider operates six data centres: two in the EEA; two in North America; and two in Asia.

The technical implementation of the cloud service means that data may be distributed across any one of the six data centres.

The cloud provider is able to provide appropriate assurances that no single data centre is likely to contain a complete and intelligible copy of the cloud customer's data. The cloud provider has also stated the location of each of the data centres.

The data will remain within the cloud provider's own network of data centres. Security will be assured through a regular independent assessment.

87. Cloud customers should remember that a foreign law enforcement agency may have the power to require cloud providers to give them access to personal data or disrupt the availability of the personal data to cloud customers and users.

88. If a cloud provider is required to comply with a request for information from a foreign law enforcement agency, and did

comply, the ICO would be likely to take the view that, provided the cloud customer had taken appropriate steps to ensure that the use of the cloud services would ensure an appropriate level of protection for the rights of data subjects whose personal data would be processed in the cloud, regulatory action against the cloud customer (in respect of the disclosure of personal data to the foreign law enforcement agency) would not be appropriate as the cloud provider, rather than the cloud customer, had made the disclosure.

89. Regulatory action against the cloud provider, in its role as data controller when disclosing data to the enforcement agency, would also be unlikely provided the disclosure was made by the cloud provider in accordance with a legal requirement to comply with the disclosure request by the agency.

Multi-tenancy environment

90. A single cloud provider may act as a data processor for many cloud customers and, in turn, may support a very large number of cloud users. This efficient use of computing resources gives rise to many of the cost savings which cloud computing can deliver. However, the result is that cloud customers may find that their data is being processed on the same systems as that of other cloud providers' customers.

91. The cloud provider must have a robust set of safeguards in place to protect against the possibility of one cloud customer gaining access to another's personal data. The cloud provider will also need to ensure that the activities of one cloud customer do not impact on those of another.

Reliability and resilience

92. Using a dedicated computing provider can help safeguard against loss of service (outages) by providing a more reliable and resilient service. However, the cloud customer should consider the consequences if a cloud provider was to suffer a major fault which took it offline.

93. It might be appropriate for a cloud customer to store a copy of its data in an alternative location, to minimise the impact of an outage.

Staff training

94. A cloud customer must recognise that a switch to cloud computing can introduce a new set of data protection risks that cloud users may be unaware of.

95. The cloud provider might offer controls that enable the cloud customer to configure the security settings of the cloud service. If it does, the cloud customer must have appropriate training and procedures in place to maintain the security that these controls offer.

96. Any procedures and policies in place must be supported by an audit function, to help ensure on going compliance.

Example
A training organisation emails documents (training packs, copies of presentations etc) to course delegates. It also emails the names and contact details of delegates to the course tutor. This puts a substantial load on the email server and the organisation decides to switch to a cloud-based file sharing service rather than upgrade the email server.

The training packs do not contain personal data but the delegate list does. For this reason, the organisation decides to continue to email the delegate list to the course tutor.

A new member of staff who is unfamiliar with the file sharing service is uploading the course packs. Instead of emailing the delegate list to the course tutor, the employee also uploads this to the file sharing website. The delegate list is now publicly available.

Rights of data subjects

97. The cloud customer must ensure that a move to a cloud service still allows data subjects to exercise their rights. For example data subjects have a right of access to their personal data and the right to object to their personal data being processed for certain purposes.

Checklist

98. Have you considered the following?

Risks	Make a list of the personal data you hold and how it will be processed in the cloud.
Confidentiality	Can your cloud provider provide an appropriate third party security assessment?
	Does this comply with an appropriate industry code of practice or other quality standard?
	How quickly will the cloud provider react if a security vulnerability is identified in their product?
	What are the timescales and costs for creating, suspending and deleting accounts?
	Is all communication in transit encrypted? Is it appropriate to encrypt your data at rest? What key management is in place?
	What are the data deletion and retention timescales? Does this include end-of-life destruction?
	Will the cloud provider delete all of your data securely if you decide to withdraw from the cloud in the future?
	Find out if your data, or data about your cloud users will be shared with third parties or shared across other services the cloud provider may offer.
Integrity	What audit trails are in place so you can monitor who is accessing which data?
	Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format.
	How quickly could the cloud provider restore your data (without alteration) from a back-up if it suffered a major data loss?
Availability	Does the cloud provider have sufficient capacity to cope with a high demand from a small number of other cloud customers?
	How could the actions of other cloud customers or their cloud users impact on your quality of service?
	Can you guarantee that you will be able to access the data or services when you need them?
	How will you cover the hardware and connection costs of cloud users accessing the cloud service when away from the office?
	If there was a major outage at the cloud provider how would this impact on your business?
Legal	Make sure you have a written contract in place with your cloud provider.
	How will the cloud provider communicate changes to the cloud service which may impact on your agreement?
	Which countries will your cloud provider process your data in and what information is available relating to the safeguards in place at these locations? Can you ensure the rights and freedoms of the data subjects are protected?
	You should ask your cloud provider about the circumstances in which your data may be transferred to other countries.
	Can your cloud provider limit the transfer of your data to countries that you consider appropriate?

More information

99. This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

100. It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

101. If you need any more information about this or any other aspect of data protection, please contact us: see our website www.ico.gov.uk.