Complying with the Data Protection Acts when outsourcing to the cloud

Stephanie Pritchett, Principal at Pritchetts, delves further into the area of cloud computing and the legal implications for organisations

Cloudy, with just a ray of sunshine? The may be one meteorologically-themed way to sum up the legal blue yonder into which many Irish business are heading, as more and more firms look to reduce the overheads and inflexibility of on-site IT functions, and instead seek to outsource these functions to internet-based service providers. Following from Gary Cominsky's excellent article in *Data Protection Ireland,* Volume 4, Issue 2, entitled 'Cloud Computing and Data Protection', this article takes a look at the legal minefield surrounding data protection issues when outsourcing to the cloud.

Data protection concerns are not the only risks when your organisation's data are spread to a variety of servers across many jurisdictions, but we will not look at disclosure and discovery or export control risks in this article. Instead, we ask whether, in data protection terms, it is possible to have your head in the cloud, whilst keeping your feet on the ground?

The legal problems

There are many different types of function which can be subject to outsourcing to the cloud, ranging from straightforward IT support to payroll functions, call centres, invoice processing or document production. Whilst there are several types of arrangement which could be put in place to 'buy in' remote services, we will look at the most common situation, in which a company wishing to outsource a function contracts with a single service provider, which in turn delivers the required services to its customer by using remote resources, ranging from sub-contracted operations to simply using remote server capacity.

In most cases, the key outcome in data protection terms is that outsourcing this business function to a service provider that is supported by cloud-based third parties will mean that, unchecked, data are likely to be collected, stored and processed by potentially unknown parties, anywhere in the world.

It should therefore be obvious that this gives rise to several thorny legal issues in relation to the requirements of the Data Protection Acts 1998 and 2003 ('the Acts'). Though this is by no means an exhaustive list, these issues will most likely include the following:

- services are often provided to a business by one contractually-bound service provider, but data are actually then sent to a bewildering variety of sub-contractors on different servers throughout the world (which we will refer to generically for the purposes of this article as 'cloud providers'). The key question that follows is what law applies and to whom (i.e. who is a data controller)?
- secondly, if the cloud providers are based outside the European Economic Area ('EEA'), how can you possibly satisfy the requirements under section 11 of the Acts — in relation to the transfer of data outside the EEA, and under sections 2(1)(d) and 2 (C) of the Acts — in relation to data security and the use of data processors, if you do not know who is handling your data and what levels of data protection they can offer?
- cloud providers usually do not have any form of direct contractual relationship with the business making use of their services through another party. There is, therefore, no straightforward way to impose standards of data security etc. on these parties by way of contractual obligations. What can be done in this situation?
- closer to home, you will need to be sure when taking a decision to outsource a business function to the cloud that you have taken the

(Continued on page 4)

Stephanie Pritchett leads the training course, 'Data Protection Essential Knowledge — Level 2' — for further details, visit: www.pdp.ie

(Continued from page 3)

necessary steps to allow this to be done in compliance with the Acts, including provision of appropriate fair processing information to data subjects and compliance with the fair processing conditions under the Acts. You will also need to consider if you need consent from all existing employees or customers if you are taking an outsourcing decision, which could be extremely onerous in terms of time and cost.

The ways forward

One of the most important steps a business can take to mitigate its potential risk is to be prepared. There is no reason why, if done carefully, use of cloud functions cannot be of great benefit to a business, whether in terms of reduced cost (particularly if the service is only billed to the extent that it is actually used rather than being a fixed overhead), increased flexibility, ease of customer or stakeholder access and in many cases, additional security against data loss or corruption.

It is, however, extremely important to undertake a careful analysis of some key issues in order to properly uphold the principles of the Acts and, where possible, to implement best practice, which is clearly an ongoing evolution.

Who is the data controller?

Firstly, in order to assess what obligations apply, it is important to understand which parties might be data controllers in any given cloud arrangement. It may be, for example, that the only data controller is the customer which originally collected the data and is outsourcing the processing function.

In some cases, however, the service provider or cloud provider can also be a data controller. Detailed analysis of this point is beyond the scope of this article, but this question will depend on a careful assessment of the exact nature of the service that is being provided to the customer. An example given by the Article 29 Working Party on Data Protection ('the Working Party') (on which more below), discusses a situation in which an online calendar system is being provided to a business for the benefit of its employees. If the cloud service provider offers some value added input, such as by offering synchronisation of online diaries, schedules or itineraries, they will be deemed to be a data controller jointly with its customer business. For a more detailed explanation of the distinction between 'data controller' and 'data processor', see *Data Protection — a practical guide to Irish and EU law* by Peter Carey (Round Hall 2010).

What law applies?

The key provision to consider here is Article 4(1) of the European Data Protection Directive from which the Irish law is derived: "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."

Helpfully, the Working Party has recently published an opinion paper ('Opinion Paper') on what law is applicable in certain situations, and its analysis includes cloud computing scenarios. It also sheds a great deal of light on the tricky issue of who is the data controller in certain situations. This Opinion Paper merely helps to clarify existing law and practice rather than creating new obligations, but it is nonetheless a welcome tool.

It is well-established then that an Irish business seeking to outsource functions to the cloud will itself be a data controller.

If so, its 'establishment' for the purposes of Article 4(1) is likely to be where the customer's offices and its physical and human resources are based (i.e. there is more there than simply a server location).

Where a service provider (and where appropriate its cloud based sub-contractors) is a data controller, then it will be necessary to determine where its establishment is — for example, does the provider have its physical servers and IT infrastructure in the EEA? If so, it will be governed by the national law in that particular jurisdiction. Recital 19 of the Directive indicates that an 'establishment' requires "the effective and real exercise of activity through stable arrangements". The European Court of Justice has stated that a stable establishment requires that "both human and technical resources necessary for the provision of particular services are permanently available."

Care must also be taken in relation to the operation of Article 4(1)(c), which is designed to impose obligations where the data controller is not based in the EEA, but where its processing of data has an obvious connection to a particular Member State. It says: "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where…the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."

There are clearly implications here for cloud computing, and again, it will be important to understand (before entering into such arrangements) whether that controller 'makes use of equipment' in a Member State. Where any doubt exists, it is likely to be a sound strategy to measure up to EU standards if possible, but the Opinion Paper does propose to limit the impact of this to data controllers outside the EU which are proactively targeting EU citizens for their personal data.

For further reading, the Opinion Paper can be found here:

http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf

Compliance with sections 2(1)(d), 2(C) of the Acts

There are obviously many potential aspects of the Acts that need to be considered, but the main risks are likely to relate to data security and potentially to data transfers outside the EEA.

Sections 2(1)(d) of the Acts states that: 'A data controller shall, as respects personal data kept by him or her, comply with the following provisions: (d) appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'

Section 2(C) of the Acts goes on to state that in considering compliance with section 2(1)(d) above, the data controller should:

- consider the state of technological development and the cost of implementing the security measures and shall ensure that the measures provide a level of security appropriate to (a) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and (b) the nature of the data concerned;
- take all reasonable steps to ensure that all persons employed by him or her and any other persons at the place of work concerned are aware of and comply with the relevant security measures taken; and
- where processing is carried out by a data processor on behalf of the data controller, (a) ensure that the processing is carried out under a contract made or evidenced in writing, (b) that the processing is only carried out on the instructions of the data controller, (c) that the processor complies with obligations equivalent to those imposed on the data controller by section 2 (1)(d) of the Acts, (d) ensure that the processor provides sufficient guarantees in respect of the technical and organisational security measures taken, and (e) takes reasonable steps to ensure compliance with those measures.

"If the cloud service provider offers some value added input, such as by offering synchronisation of online diaries, schedules or itineraries, they will be deemed to be a data controller jointly with its customer business."

Compliance with these principles and section 11 of the Acts (discussed below) seems like a particularly tall order in cloud computing scenarios, where a business that has collected personal data may not have a direct contractual relationship with data processors or even other data controllers in any given arrangement. One must therefore at least employ sensible practical measures to mitigate the risks that this presents.

Investigation

In essence, it is necessary find out what you can about the companies with whom you are contracting, and about their sub-contracted providers to the extent that this is possible. You should make written enquiries (and document the responses) on such matters as:

(1) To whom are data being sent, and where are these parties based?

(2) where are data physically stored?

(3) if data are being sent to the US, whether any party is Safe-Harbor registered?

(4) what security and disaster recovery policies are in place? Do you require more stringent measures?

(5) what are the back-up procedures, both in terms of information recovery and in term of the location of backed-up data?

(6) are encryption technologies used?

(7) how are data kept distinct between different customers?

(8) can the service and cloud provider comply with any relevant industry specific regulatory requirements?

(9) what personnel will have access to the data? Have they been vetted?

(10) do the service and cloud providers have a good compliance history?

In practical terms, a good cloud business should have a working knowledge of Irish and EU data protection requirements and should be able to offer the following to provide a far greater degree of certainty:

- sufficient due diligence information; or
- services that are restricted to certain jurisdictions (e.g. Ireland or the EEA).

There are already cloud providers offering restricted transfer services (such as 'Europe Only') which would mitigate many of the risks of non-compliance with section 11 of the Acts. From a business' perspective, you should be wary of engaging the services of a company which is unwilling or unable to provide the type of due diligence information referred to above or to divulge where data will be stored and processed.

(Continued on page 6)

(Continued from page 5)

Contractual arrangements

Having ascertained the answers to the above questions, there should be some scope not only to make an informed decision about the arrangements (and check what consents may be necessary — see below), but there may also be an opportunity to impose more robust contractual obligations on service providers in relation to data protection and security issues, beyond those legally required under section 2(C) of the Acts.

Such contracts could helpfully address issues such as the following:

(a) precise description of the nature of the services provided;

(b) what instructions are given to the provider (and importantly, what can they not do?);

(c) ensuring the security of any data and requiring appropriate segregation from those of any other customers;

(d) reporting obligations for data loss incidents;

(e) requirements in relation to subject access requests;

(f) what warranties the providers will give in relation to the processing of personal data in the cloud;

(g) ability for customers to impose further security and processing requirements in the event of changes to data protection law;

(h) termination provisions and requirements to destroy data; and

(i) ability for customers to audit the provider's policies and procedures.

Solid contractual provisions, targeted specifically at the risks that your due-diligence exercise has highlighted, will go a long way to demonstrating compliance with the relevant sections of the Acts.

"Where the service provider or cloud providers are based in a foreign jurisdiction with levels of data protection which are not as great as Ireland, customers and employees should be made aware of this."

Compliance with section 11 of the Acts

Section 11 of the Acts requires that: "The transfer of personal data to a country or territory outside the EEA may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer…"

Transfers of personal data outside the EEA are therefore prohibited, unless adequate compliance measures are taken. A full analysis of the pros and cons of the respective compliance measures is beyond the scope of this article.

Suffice to say, as data controller, the customer will usually be required to ensure compliance with section 11 where due diligence shows that the data may be sent to various jurisdictions within the cloud.

As only Andorra, Argentina, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey and Safe Harbor-certified American corporations have been designated as 'safe' areas for transfer, other compliance routes will often need to be pursued.

One means of compliance would be to obtain consent from all the data subjects affected (written consent if sensitive personal data are to be transferred), though this will be difficult in practice as it can be hard to show that the consent was 'freely given, specific and informed' and problems arise when consent is withheld or withdrawn.

As binding corporate rules do not yet appear to be an effective compliance measure, data controllers will often therefore look to a contractual compliance solution, such as requiring the service provider and each cloud provider to execute the European Union approved standard contractual clauses for data processors which will require the service provider to effectively commit to complying with EU-equivalent standards.

Provision of fair processing information

The outsourcing entity as data controller will need to ensure that the data have been collected and processed fairly, as required under sections 2(1)(a) and 2D of the Acts. Essentially, people that the outsourced data relate to need to be told what uses the data are to be put to, and what disclosures might be made. In particular, where the service provider or cloud providers are based in a foreign jurisdiction with levels of data protection which are not as great as Ireland, customers and employees should be made aware of this.

Data subjects should be told about the proposed processing, including:

- that their data are to be processed by a third party, and if relevant, any sub-processors;
- that their data are to be processed by a third party cloud-based service provider;
- the purposes for which the third parties will process their data;
- that they have the right to access data and have it erased; and
- whether any information is to be transferred or processed outside the EEA, and if so what steps have been taken to ensure compliance with the Acts, and details of someone to whom enquiries can be directed.

It is, therefore, self-evident that in order to provide this information to

data subjects, you need to know it yourself, which again highlights the need for a detailed due diligence approach.

It is, of course, straightforward enough to provide new customers or employees with a data protection notice at a stage when you are already considering outsourcing. It is another matter entirely trying to provide this notice to a huge number of existing data subjects.

Section 2D(1)(b) requires such a notice to be issued "so far as practicable", with an exemption that may apply where complying would involve 'disproportionate effort'. It is tempting to see this exemption as an easy get-out, but extreme care should be taken if seeking to rely on it. Administrative cost, extra management time and some degree of business interruption may not be seen as enough to demonstrate 'disproportionate effort', so it is best to consider that a notice should be given in all but the most extreme circumstances.

Compliance with fair processing conditions

Except where a relevant exemption applies, the Acts (under sections 2A and 2B) also require that the data controller must be able to legitimise the processing of personal data by the service provider and cloud providers before any processing of personal data are carried out. If only non-sensitive personal data are to be transferred into the cloud, then one of the following conditions may be relied on:

- consent;
- necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract;
- necessary to comply with a legal obligation of the data controller — other than a contractual obligation;
- necessary to prevent injury or other damage to the health of the data subject or to prevent serious loss or damage to the property of the data subject or to protect the vital interests of the data subject;
- necessary for certain public function reasons; and
- necessary for the legitimate interests of the data controller or a third party to which the data are disclosed, except where it is unwarranted because it is prejudicial to the data subject.

Where sensitive personal data are also to be transferred into the cloud, an additional condition (as set out under section 2B of the Acts) must be met. While there are a number of potential conditions, obtaining explicit unambiguous consent of data subjects will often be used, though this can be difficult to obtain in practice.

A detailed analysis of the applicability of the various conditions is beyond the scope of this article but the data controller will need to satisfy itself as to which condition(s) it intends to rely on before making any transfer of information to the service and cloud providers.

Conclusion

Whilst there are undoubtedly a far greater number of data protection considerations to address when outsourcing to the cloud, none of the issues are insurmountable, and as cloud-based providers become more sophisticated in response to customer demand, the legal issues should be easier to address. The Opinion Paper is also extremely welcome and provides a reasonably pragmatic (and some might say conciliatory) approach to questions over applicable law and who is to be considered to be the data controller.

With careful consideration, the potential cost savings and accessibility benefits can quickly outweigh the extra compliance burden, and with careful planning, specialist data protection involvement from an early stage and a willingness to the see the compliance issues as a potential selling point for customers rather than a compulsory irritation, a leap into the cloud could precipitate great business success.

Stephanie Pritchett
Pritchetts
stephanie@pritchettslaw.com