The 10 commandments of data privacy in outsourcing contracts

Bojana Bellamy, Global Data Privacy Compliance Lead at Accenture, discusses the key privacy elements of outsourcing contracts and the challenges presented by international data transfers, especially from the EU to countries without adequate privacy protection.

Companies are increasingly turning to offshore outsourcing to reduce the costs of their non-core functions. Many offshore outsourcing service providers are located in countries with minimal or no data protection laws, such as Brazil, Russia, India and China. As such, the contracts entered into between data controllers and data processors are of critical importance to the protection of data and individual privacy.

Data protection is a vital issue in the outsourcing business and has implications at social, legal, financial and political levels. It is also a major international issue as outsourcing is not always onshore but off-shore relative to the company that owns the data. Many companies who provide outsourcing services are located in countries without data protection laws, yet the companies they serve are often located in privacy regulated countries. The lack of consistent national privacy standards means that the contracts that companies enter into in an outsourcing transaction are critical to ensure that the parties understand their obligations in relation to the data being transferred and outsourced.

Data controllers and data processors in outsourcing

Outsourcing is the process in which a principal (a data controller) hands over the administrative processing work of a particular function to a third party agent (a data processor) in exchange for a fee (or other incentive). The data controller determines the purpose and means of processing data, which the data processor executes on their behalf.

The data controller remains responsible for compliance with applicable privacy laws and the appropriate data security measures that the data processor needs to implement. The data processor is then responsible for the implementation of the data security measures. This would include the technical and organisational measures to protect against unauthorised and unlawful disclosure, access, alteration, destruction or loss of data.

Table 1: Why outsource?

To reduce and control operating costs	17%
To improve company focus	**16%**
to gain access to world-class capabilities	12%
To free resources for other purposes	**12%**
Resources not available internally	8%
To reduce time to market	**6%**
To take advantage of off-shore capabilities	6%
To accelerate the benefits of re-engineering	**4%**
To share risks	3%
The function is difficult to manage or out of control	**3%**

Table 2: Top 10 functions that are outsourced

Human resources	7%
B2B & B2C customer relationship management	**6%**
Distribution and logistics	3%
Administration	**3%**
Manufacturing	2%
Facilities management	**2%**
Finance	1%
Full IT outsourcing	**1%**
Transportation	1%
Sales and marketing	**0%**

Data controllers outsource non-core business functions to data processors primarily to reduce costs. The Outsourcing Institute surveyed 1,410 of its new members in 2005 to ascertain the top 10 reasons why companies outsource. These are shown in table 1.

The types of functions typically outsourced include IT applications and infrastructure, and business processes. IT application outsourcing generally involves the management of software, such as SAP, PeopleSoft and Oracle. IT infrastructure outsourcing includes data centre services, such as hosting applications, storage and helpdesk services. Typical business processes that are outsourced are human resource and customer relationship management functions.

The same survey found the top 10 functions that are outsourced. These are shown in table 2.

The 10 commandments

The increased risks to data privacy that naturally arise due to the handing over of data to a third party and subcontractors, who may be offshore, means that data controllers and data processors

Table 4: Controller's options if transferring data out of EU

• Transfer of personal information with the individual's consent	**Difficult to achieve**
• Transfer under Safe Harbour principles	**Only relevant to transfers to the USA**
• Authorisation by national data protection supervisory authority	**Process too long**
• Using EU Model Clauses	**Best option**

should focus on ways to minimise that risk. This can form the basis of the contract between the data controller and the data processor. Indeed, several countries, including EU countries, the US, Canada, Hong Kong and Japan, require data controller and data processor to have a written agreement before data transfer takes place. The top 10 data privacy elements to consider when forming an outsourcing agreement are outlined in table 3. Some of these may also be considered pre-contractual steps.

International data transfers

EU data protection laws prohibit the transfer of personal information from the EU to countries outside the EU that do not have an adequate level of data privacy law. The EU has declared that Switzerland, Argentina, Canada, the Isle of Man, Guernsey and Jersey have adequate levels of data privacy law. In countries that the EU considers not to have adequate levels of data privacy law, such as Brazil, Russia, India and China, a data controller in the EU that wishes to transfer personal information to those countries must comply with the requirements regarding international data transfers. The main options that a data controller can consider in outsourcing to a country without an adequate level of data privacy law are shown in table 4.

In December 2001, the EU adopted a standard contract (EU Model Clauses) that data controllers can use to transfer personal information to data processors in countries without adequate data privacy laws. This needs to be submitted to (though not approved by in most cases) the national data protection supervisory authority. The consent of individuals for the transfer is not required. However, if sensitive personal information is being transferred, then individuals must be notified.

Conclusion

Outsourcing a company's functions to a third party inherently increases the risk to data privacy and security. The risk is further increased when the data is transferred offshore. However, when data controllers and data processors are able to clearly define each of their responsibilities in terms of data privacy and security, then that risk is reduced.

The 10 commandments of data privacy in outsourcing contracts as outlined in this article assist data controllers and data processors to focus on and address the privacy implications of the transfer of data.

AUTHOR

Report by Annelies Moens.

Table 3: Top 10 data privacy elements to consider

1 **Define the roles and responsibilities of the data controller and data processor**
2 Define the security policies and procedures applicable to the data controller's data
3 **Outline the data controller's right to audit the data processor's premises, policies and procedures**
4 Check the reliability of the data processor's staff and their awareness of privacy issues
5 **Define who is responsible for the access, correction and removal of personal data**
6 Outline the process for regulatory investigations, complaints handling and enforcement measures and who bears the costs
7 **Outline the processes for dealing with regulatory changes**
8 Consider the steps required for international transfer of data
9 **Develop procedures to be taken in the event that a data security breach occurs, including notifying individuals where this is required or deemed appropriate**
10 Consider international data security certification standards, such as ISO17799