IT Law from a Practitioner's Perspective

Agne Lindberg & Daniel Svensson

1 Introduction …….. 12

2 Cloud Computing ……. 12
2.1 What is it? ……..... 12
2.2 Basic Cloud Architecture and Service Models ……..... 13
2.2.1 Software as a Service (SaaS) ……...…. 14
2.2.2 Platform as a Service (PaaS) ……...…. 14
2.2.3 Infrastructure as a Service (IaaS) …….. 15
2.3 Essential Characteristics of Cloud Computing ……...…. 15
2.4 Legal and Contractual Issues in the Cloud ……... 17
2.4.1 Assigning the Data Controller ……...…….. 17
2.4.2 Security Requirements ……...…….. 18
2.4.3 Cross Border Issues ……... 18
2.5 Traditional Outsourcing vs Cloud Computing ……...…… 19

3 Trends in Outsourcing ……..…… 20
3.1 Introduction …… 20
3.2 Customized Agreements ……...…. 20
3.3 Service Levels ……...…… 20
3.4 Transition and Transformation Projects ……. 20
3.5 ITIL ……...……. 21
3.6 Cloud Computing ……...…… 21
3.7 Offshoring ……...…... 21
3.7.1 Introduction ……...… 21
3.7.2 Factors to Consider when Selecting Offshoring Destination …… 22
3.7.3 Contractual Considerations ……...… 22

4 New Standard Clauses for Transfer of Personal Data ……. 23
4.1 Introduction ……..……. 23
4.2 The New Standard Clauses ……...……. 23
4.3 Need for Additional Standard Clauses? ……...…….. 25

5 Recent Case Law Developments ……. 26
5.1 The Pirate Bay …… 26
5.1.1 Introduction ……...…… 26
5.1.2 Overview of the Legal Issues …… 26
5.1.3 The Ruling ……...…. 28
5.1.4 Implications of the Pirate Bay Case ……..…….... 28
5.2 Google AdWords ……...…… 29
5.3 Personal Data on Facebook and Other Social Media ……. 29
5.3.1 Introduction …….. 29
5.3.2 Recent Decisions by the Swedish Data Inspection Board ……..... 30

1 Introduction

During the last decade, the rise of virtually new technological and organizational phenomena, such as cloud computing, virtualization, off- and nearshoring, e-commerce and social media (and other websites including user-generated content) has dramatically changed the scene and the conditions in which IT law is being practiced. However, an ever-changing working environment will come as no surprise for IT law practitioners, who over the years have become used to such rapid developments. In fact, one could even suggest that the only constant within this particular field of law is its continuing change!

In order to successfully practice IT law, it is vital to acknowledge that legal considerations, analysis or even democratic process is very rarely the catalyst for legal development within this branch of the law. Rather, such development is generally driven through technological break-troughs as well as development of new and/or different business models of the suppliers and other stakeholders in the business. Any judicial review or implementation of specific legislation for a technology or business model phenomenon will generally take years to complete. This means that, as an IT lawyer, you will regularly find yourself playing catch-up with the ideas, concepts and ambitions of software developers, IT architects, engineers and other technicians in order to keep up with and – to the best of one's ability – comprehend the products, services and business models which are currently subject to legal analysis. In our experience, it is almost impossible to successfully draft and interpret the extensive and very detailed IT agreements that are common practice in today's IT market if you do not understand the fundamentals of the underlying technology and business models.

Consequently, we consider IT law practitioners to have an important function as an intermediary between the rapidly changing world of IT and the (somewhat less agile) legal society. This article will, from the perspective of a legal practitioner rather than that of a legal scholar, highlight and discuss current trends as well as recent developments and changes within the IT sector. We have chosen to focus on four separate areas, namely cloud computing (Chapter 2), trends in outsourcing (Chapter 3), new standard clauses for transfer of personal data outside EU/EEA (Chapter 4) and recent case law developments (Chapter 5). With these subject areas, we believe we cover the bulk of issues that arises in a daily IT-law practice.

2 Cloud Computing

2.1 What is it?

Although cloud computing has been something of a buzz word within the IT industry for a number of years, there is still an on-going debate on how to accurately define the concept. In fact, leading IT consultancy firms such as the Gartner Group, McKinsey & Co. and Forrester along with service providers such as Google, Salesforce.com and Amazon all promote their own definition of the term. According to a 'white paper' published by McKinsey & Co in 2009 there are 22 different definitions of the term (or actually 23, since the report also

includes McKinsey & Co's very own definition).[1] However, perhaps the predominant definition is the one provided by the U.S. National Institute of Standards and Technology (NIST):

> "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [2]

As indicated in NIST's definition, cloud computing typically involves over-the-Internet provision of scalable and often virtualized resources. As opposed to traditional applications which are installed locally at the user's own computer, cloud services will generally take the form of web-based tools or applications that users can access and use through a web browser or another web service.

With regard to the use of the metaphor 'cloud', this term has actually been taken from the telephony industry that in the 1990s began shifting from point-to-point data circuits to Virtual Private Network (VPN) services. A cloud symbol was then used to denote the demarcation point between the responsibilities of the provider and the user.[3] Perhaps Google CEO Eric Schmidt describes the cloud metaphor more eloquently:

> "What [cloud computing] has come to mean now is a synonym for the return of the mainframe,…and the mainframe is a set of computers. You never visit them, you never see them. But they're out there. They're in a cloud somewhere. They're in the sky, and they're always around. That's roughly the metaphor."[4]

2.2 Basic Cloud Architecture and Service Models

The two basic components of the architecture used for delivery of cloud services are generally referred to as the 'back end' and the 'front end' of the services. The 'back end' of the cloud computing architecture is the 'cloud' itself, consisting of computers, servers and data storage devices hosted by the service provider. In practice, the back end systems for cloud service providers will be located at large centralized data centers hosted and maintained by the service provider. The 'front end' of a cloud computing architecture is the part seen by the user. This includes the network (or the computer) and the applications and interfaces used to access the cloud service, such as web browsers.

Another way of describing cloud computing is through the shift towards 'as-a-service'-solutions. Rather than the customer purchasing its own IT

---

1 McKinsey & Co. report: "Clearing the Air on Cloud Computing", available for download to registered users of "www.uptimeinstitute.org ".

2 The NIST Definition of Cloud Computing, Version 15, 10-7-09, written by Peter Mell and Tim Grance (available for download at "csrc.nist.gov/groups/SNS/cloud-computing").

3 One of the earliest documents in which the term "cloud" was used is a meeting report from a working group (ATM) of the IETF in 1993, which is available for download at "mirror.switch.ch/ftp/doc/ietf/ipatm/atm-minutes-93jul.txt".

4 The quote is from an interview that was published by Businessweek journal in 2007, *see* "www.businessweek.com/magazine/content/07_52/b4064052938160.htm".

infrastructure and/or software licenses, such products are provided by the service provider 'as-a-service' to the customer. With regard to cloud services[5], such will typically include delivery of software, infrastructure and storage over the Internet.

There are three main service models for cloud services, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). All these service and business models share the basic characteristics described below.

2.2.1 Software as a Service (SaaS)

The capability provided to the customer through SaaS is the possibility to use the service provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. [6]

SaaS is a broad market, and services can include anything from rather simple web-based email solutions to complex Customer Relationship Management Systems. The process towards SaaS has been driven not only by suppliers, who can decrease costs for distribution and maintenance, but also by customers, who prefer not to handle issues regarding licensing and hosting of the software. A SaaS-contract will focus less on the right to use the service (or license if applicable), and more on functional service descriptions, services levels (e.g. availability and maintenance requirements), service level remedies (e.g. liquidated damages) and exit management provisions to ensure co-operation and transfer of data upon the termination or expiration of the SaaS-contract. The extent of actual copyright use in SaaS-structure (and hence the need for an explicit license provision in a SaaS-contract) is debatable. In our opinion, it depends on the technical solution and whether the end user is duplicating the software when using the software. Normally, SaaS-solutions involve complex licensing issues between the developer of the applications and the service providers. New licensing models have been developed to provide for SaaS-solutions.

2.2.2 Platform as a Service (PaaS)

The capability provided to the customer through PaaS is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider. The customer does

5 It should be noted that the trend towards distribution 'as-a-service' is not limited to cloud services on the Internet. Many hardware manufacturers (e.g. of computers and printers) provide 'as-a-service' options for its customers. Such options typically include services like financing and maintenance and are billed through subscription or a utility-based fee structure.

6 The NIST Definition of Cloud Computing, Version 15, 10-7-09, written by Peter Mell and Tim Grance (available for download at "csrc.nist.gov/groups/SNS/cloud-computing").

not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.[7]

PaaS facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.[8]

2.2.3 Infrastructure as a Service (IaaS)

The capability provided to the customer through IaaS is the possibility to provision processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).[9]

Similar to most cloud services, IaaS is typically billed on a utility computing basis and amount of resources consumed rather than availability to a certain infrastructure (for example server model, processor type etc), meaning that the cost will reflect the level of activity on the infrastructure.

2.3 Essential Characteristics of Cloud Computing

In our opinion, the benefits of cloud computing compared to traditional service delivery models are quite obvious. For the service provider, a cloud service delivery optimizes the utilization of resources and decreases cost. For the customer, a cloud service avoids the need for large investments in hardware, software and services and enables the customer to pay on a utility (cost per resources consumed) or subscription (time-based cost) basis with little or no upfront cost. From an accounting perspective, this also means that customers can convert capital expenditure to operational expenditure – moving from fixed to flexible costs.[10]

More specifically, the following aspects are generally considered as essential characteristics of cloud computing.[11]

On-demand self-service. A customer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs). This also means that most cloud services are device and location independent since users can connect from anywhere using the device of his or her choice.

---

7 *Ibid.*

8 *See* "aws.typepad.com/aws/2008/06/the-forthcoming.html".

9 *See* the NIST Definition of Cloud Computing, Version 15, 10-7-09, written by Peter Mell and Tim Grance (available for download at "csrc.nist.gov/groups/SNS/cloud-computing".

10 *See* "www.cloudave.com/link/recession-is-good-for-cloud-computing-microsoft-agrees".

11 *See* the NIST Definition of Cloud Computing, Version 15, 10-7-09, written by Peter Mell and Tim Grance (available for download at "csrc.nist.gov/groups/SNS/cloud-computing".

Resource pooling. The service provider's computing resources are pooled to serve multiple customers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. This also enables a high level of customization and creation of a customer-defined experience of the service. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the service provider and the customer of the utilized service. This is of essence to create more utility based business and payment models.

In addition to the characteristics described above, one could also argue that a cloud service will *facilitate maintenance* of the services as well as increase the level of *information security*. In terms of maintenance, cloud computing applications are easier to maintain since they don't have to be installed on each user's computer. This of course means that updates, upgrades or fixes can reach all users instantly and without the need for multiple installations.

The argument that cloud computing services will increase the level of information security is more contentious. The basis of this argument is that the service provider will have increased possibilities to retain control over both physical and network security due to the centralization of data. In addition, cloud service providers will be able to devote more resources to security issues than many customers are able or willing to afford. Another argument is that the complexity of security is greatly increased when data is distributed over a wider area and number of devices (so-called data segregation). In spite of these possible advantages from a security perspective, many customers remain hesitant to store valuable or sensitive data with a cloud service provider and prefer to store such data at the customer's own locations. In fact, it seems that information security is one of the most contentious issues in relation to cloud computing (see section 2.4 below). Only time will tell to what extent cloud service providers will be able to convince customers that information security will not be compromised due to off-site (cloud) storage. In this respect, we believe it is likely that new security standards and certification procedures will be established enabling service providers to can obtain an 'objective' level of information security in the cloud.

2.4 Legal and Contractual Issues in the Cloud

The introduction of cloud services has undoubtedly caused some debate within the IT legal society. As already indicated above, the legal implications of the information security risks were among the first causes for concern. In fact, one of the most frequent points of negotiation in relation to a cloud services contract is the level of liability that the service provider is willing to assume for the data which is stored and hosted by the service provider. Despite the alleged advantages to information security when using cloud services (see section 2.3 above), we find that service providers tend to be surprisingly unwilling to assume a corresponding level of contractual liability for the hosted data. In our opinion, industry practice in Sweden when it comes to responsibility for hosted data is limited to an obligation for the provider to perform regular back-ups and that the customer can only claim compensation for lost data if and to the extent the service provider has breached its back-up responsibility. In addition, many service providers will attempt to define loss of data as an 'indirect' loss, which in effect means that the provider would only be liable for loss of data in cases of gross negligence or willful misconduct.

Further, the issues surrounding personal data in relation to cloud services have been frequently discussed between IT lawyers. Many, or perhaps most, cloud services will to some extent include processing of personal data (such as names, addresses, IP addresses etc). In Sweden, the legal framework to consider in this respect is mainly the Data Protection Directive[12] and the Swedish Personal Data Act (1998:205). In relation to cloud services, there are at least three separate issues to consider with regard to personal data processing.

2.4.1 Assigning the Data Controller

Firstly, it is crucial to consider who – under the specific cloud service – should be considered as the data controller (i.e. the person which alone or jointly with others determines the purposes and means of the processing of personal data). A cloud service provider will typically want to avoid assuming the role of a controller, but rather act as a data processor (i.e. as the person who processes personal data on behalf of the controller). To assign these roles may come across like an easy task, but in many cases this issue will require careful legal considerations as well as detailed technical specifications of the relevant cloud service (see also section 5.3 below). Under the personal data legislation, a data controller will have several obligations which the processor does not have (e.g. to ensure legality and legitimacy of the data processing and, if required, collect consents from the individual subjects). Although correctly assigning the data controller can be a complex task, it should be noted that most established cloud service providers have designed their services to ensure that the customer retains the role and responsibility as data controller, meaning that the cloud service provider will act as a data processor.

12 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2.4.2 Security Requirements

Under Article 17 of the Data Protection Directive and 31 § in the Swedish Personal Data Act, the data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access to personal data. According to 30 § Personal Data Act, when the data controller engages a data processor through the purchase of cloud services, such a relationship must be governed by a written agreement that includes an explicit obligation for the processor to implement security arrangements that fulfill the requirements set out in personal data legislation. The processor must also be obliged to adhere to any and all instructions from the controller regarding the personal data.

These obligations mean that the customer of cloud services must typically (i) carry out a due diligence of the security measures provided by the provider, (ii) take reasonable steps to ensure compliance with those measures, and (iii) ensure that the contract includes the required obligations for the cloud service provider. Important documentation to review for the customer includes the provider's security policies (physical, network and server security as well as data segregation and encryption policies), audit/certification capability information and statements on accounting standards (e.g. SAS 70).

2.4.3 Cross Border Issues

Under the Data Protection Directive, personal data is allowed to be transferred freely within the EU/EEA area. However, transfer of personal data (including provision of access to such information) outside this area is not allowed, unless country in question ensures an 'adequate level of protection' for the personal data. The EU Commission have determined certain countries to have such adequate level of protection, namely Argentina, Canada, Switzerland, Jersey, Guernsey, the Isle of Man and the Faroe Islands.[13] In addition – and more perhaps more importantly in relation to cloud services – transfer of personal data to the US is permitted provided that the relevant US company is registered on the Safe Harbor List[14], thus certifying to meet the essential requirements of the Data Protection Directive. It should be noted that the EU-US Safe Harbor has been the subject of significant criticism regarding compliance and enforcement.[15]

For any transfer of personal data to other countries than those set out above, it is possible to use certain standard contracts/clauses issued by the European Commission (see further under Chapter 4 below). For transfers within multinational organizations, it is also possible to set up and rely on specific

13 The EU Commission is currently considering whether also the data protection in Andorra and Israel should be considered 'adequate'.

14 *See* "www.export.gov/safeharbor/".

15 For example, see the report "The implementation of Commission Decision on the adequate protection of personal data provided by the Safe Harbor Privacy Principles (2004)", issued by the European Commission and published at "ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf ".

Binding Corporate Rules (BCR). In Sweden, the use of BCR must be approved in advance by the Swedish Data Inspection Board.[16]

In order to assess the cross border issues involved in a cloud service, it is imperative for the customer to have information on the actual flow of information. Simply put: you must know where the data is throughout the entire service.

2.5 Traditional Outsourcing vs Cloud Computing

From the perspective of a potential customer of cloud services, it could be argued that a shift from using internal resources (e.g. its own platform or software licenses) to purchasing such resources from a cloud service provider is in fact nothing more than a sourcing issue. In fact, we would suggest that the choice is identical to that of outsourcing; the issue to consider is whether to purchase the products or services externally or to produce, manage and/or maintain it yourself internally.

In terms of the contract structure, a cloud service agreement is essentially similar to outsourcing agreement except that a traditional outsourcing generally involves a transfer of business, personnel and assets. A shift to cloud services will typically not require any such transfer. This means that the contract for a cloud service is substantially less extensive than an outsourcing agreement. As for contractual issues like service content, service levels, exit management, audit and confidentiality, the contract types are however very much the same. As discussed above, the legal challenges and points of contract negotiation are to a large extent focused on information security and personal data issues. Another key issue for the customer is to make sure that the contractual service levels and remedies are satisfactory and can effectively be used to hold the supplier liable in case of unavailability (or other defects in the services). Further, as a customer of cloud services it is – to an even higher extent than for an outsourcing customer – vital to minimize supplier dependency. This can be achieved through careful drafting of the service descriptions (e.g. ensure compatibility with services from other suppliers) and the inclusion of adequate exit provisions (e.g. obligations for the supplier to assist in transfer to a successor supplier) as well as benchmark possibilities to ensure market prices over a longer term.

To summarize, a cloud service typically involves fewer legal considerations than a service provisioning through traditional outsourcing. The similarities between the two are however apparent since both phenomena are, in essence, nothing else than a complex service delivery. Many of the negotiation points in a cloud service contract will therefore be similar to those in outsourcing agreements.[17]

16 *See* "www.datainspektionen.se/om-oss/internationellt-arbete/tredjelandsoverforing/#13".

17 For an extensive overview of such issues, see Lindberg/Kahn/Krouthén: *IT-avtal – särskilt om outsourcing*, Norstedts Juridik, 2009.

3 Trends in Outsourcing

3.1 Introduction

It is clear that the nature of outsourcing contracts, and IT agreements in general, has substantially changed over the last twenty years. Whereas such agreements used to focus primarily on delivery of hardware and descriptions of the technology used, they today tend to focus on services, software, business efficacy, functionality and end-to-end responsibility for the supplier. Obviously this means that also the drafting of IT agreements has changed substantially. This chapter will elaborate upon this development, and briefly describe the most prominent trends with regard to such developments.

3.2 Customized Agreements

The customer today tends to draft essential parts of the agreement, for instance the conditions concerning main terms and conditions (such as confidentiality, force majeure, limitation of liability, term and termination as well as dispute resolution), exit management, audit, liability etc, whereas the parties tend to jointly draft service descriptions, service levels and pricing models in order to achieve a service delivery that corresponds to the supplier's standards and thus ensures a price-efficient delivery. As a consequence, the customer nowadays takes on the task of analyzing the needs and purposes of the agreement to a higher extent than before. It should in this context however be noted that such analysis might prove to be difficult for a first-time customer, and that such customers will inevitably rely on the supplier to a higher extent than more experienced customers.

3.3 Service Levels

With regard to service levels, there is a clear trend towards combining traditional IT-oriented service levels (such as availability of a particular server or WAN) with more user or effect oriented levels, sometimes called Business Level Agreements (BLAs). The starting point for such BLAs is not the technology and how it meets certain requirements, but rather how the customer's business can use the services delivered. An example of BLA is time-to-market, i.e. the time elapsed between a customer's request for a change until such new product or service can be sold on the market by using the supplier's services. The increasing importance of BLAs is partly caused due to customers being unsatisfied with traditional remedies for service level defaults (e.g. monetary penalties). Such remedies are still being used, but they are more and more focusing on the service levels and areas that are of very high importance to the operations of the customer.

3.4 Transition and Transformation Projects

The actual success of an outsourcing project is largely dependent on the success of the transition project (the project for transferring delivery of the services to the supplier with a focus on "as-is" delivery) and the transformation project (the project for transforming the structure of the delivery to a future mode of delivery). There are many examples of disputes in relation to outsourcing agreements projects which have been caused by unsuccessful transition and/or

transformation projects. Therefore, these projects are nowadays specifically and extensively set out in the agreement, including clear descriptions of the projects the parties' responsibilities and a detailed timetable. For instance, the supplier's delay is often subject to penalties and the agreement often entails a possibility for the supplier to terminate the agreement if the delay surpasses a certain period. The trend is less clear with regard to the customer's delay, but it may for example be sanctioned by a shift in the deadline for transition and the customer may be liable for some of the supplier's set-up costs, which has arisen as a result of the delay.

3.5 ITIL

To varying extents, both suppliers and customers tend to follow ITIL processes. ITIL stands for "IT Infrastructure Library" and includes a compilation of best practices gained over many years. ITIL is issued by the Office of Government Commerce, which is a UK authority responsible for public sector procurement. ITIL describes a rather general level of how to structure the working practice and the delivery of IT services in a stable and cost effective manner by controlling for instance the manner in which faults are handled, changes and long-term planning to prevent crises. If both parties are following ITIL or have processes implemented that are based on ITIL, the contract needs to be adopted to ITIL processes and terms.

3.6 Cloud Computing

It almost goes without saying that the rise of cloud computing has affected also the content and focus of outsourcing agreement, see section 3 above.

3.7 Offshoring

3.7.1 Introduction

A very clear trend is that outsourcing agreements are transnational and that resources from other countries than the customer's own country are used for service delivery. The phenomenon has different names, such as "nearshoring" if the services are supplied by countries in the customer's near surrounding and "offshoring" if the distances are longer.

The increasingly global economy enabled and facilitated offshoring. Offshore outsourcing was initially a way for the customer (and the supplier) to reduce the costs of human resources in particular. This is of course still one of the strongest driving forces, but other elements such as reduction of time-to-market and the possibility to focus on core activities are nowadays contributing reasons. Offshoring may be designed in a variety of ways, for instance in so-called captive centres, i.e. a customer-owned offshore operation. The activities in a captive center are performed offshore, but they are not outsourced to another company.

India is currently one of the largest offshoring destination in terms of IT, due to the language skills (English), highly educated personnel, relatively low costs and the fact that the Indian suppliers have a high degree of maturity in their technology and processes. Indian suppliers are however experiencing increasing competition and other geographic areas which are emerging from Asia, in particular China, Vietnam, Thailand, Malaysia, as well as Central and Eastern

Europe. From a European legal perspective, it is advantageous that many of the Central and Eastern European countries have become EU members in recent years since this facilitates many legal issues, such as transfer of personal data and other regulatory considerations.

3.7.2 Factors to Consider when Selecting Offshoring Destination

Determining the most suitable offshoring destination is obviously an important task, and when doing so the following decisive factors should be considered:

• *Cost.* For many customers, this is the most important factor and it will, needless to say, differ between countries.

• *Manageability*. One should take into account the manner in which the offshore operations are handled from the customer's location and it may often require interaction and physical meetings.

• *Quality*. The supplier's quality, competence and language skills need to be considered.

• *Risks*. Both the technical and geopolitical risks should be taken into account.

• *IT compatibility*. IT is not only a contractual object, but also crucial for a successful delivery which raises questions regarding access to communications and infrastructure.

• *Corporate Social Resonsibility (CSR)* focuses on factors such as the conditions of the staff.

• *Predictability / sustainability*. Many of the offshoring countries evolve very fast and one should consider the country's possible development and the consequences it may have on the business long term.

3.7.3 Contractual Considerations

Offshoring affects the drafting and content of the outsourcing agreement since the agreement must not only address the traditionally important issues but also the fact that multiple jurisdictions are involved. The main elements which therefore should be included in the agreement or in the contractual process are:

• *Regulatory issues.* There are three different aspects of outsourcing with regard to regulatory issues: i) the services, and the data required when delivering the service, will be moved from the customer's country, ii) such services and data will be brought into the supplier's country and iii) the service will be produced in another country. The first point may for instance raise questions regarding transfer of personal data which would require taking into account the European and national rules regarding such data transfer to third countries. Points two and three, infer that the customer need to consider which licenses and permits are required in the country of the supplier.

• *Intellectual property rights*. The IP law in the supplier's country needs to be analyzed. The agreement should of course include a clause stipulating that the supplier takes full responsibility for the any transfers of IPR envisaged in the agreement. IP law is often mandatory and efforts have been made to globally harmonize IPR, for example through the TRIPS Agreement under the World Trade Organization, which however provides less protection than many of the European countries' legislations. The outsourcing agreement should consequently contain a very clear description of IPR and the manner in which agreements with employees and subcontractors should be regulated.

• *Management of employee turnover*. The continuity of staff is important for the quality of services and the staff turnover should therefore, in countries where the staff turnover and the view thereupon differ, be measured in the context of proactive service levels.

• *Audit.* The audit clause should be drafted in a manner which enables and facilitates actual on-site audits on the supplier's and sub-contractor's premises.

• *Safety*. Offshoring is often associated with specific safety requirements which should be taken into account, for instance insurances of infrastructure.

• *Time zones*. The agreement should take into account that countries operate on different time zones why the applicable zone should be clearly regulated.

4 New Standard Clauses for Transfer of Personal Data

4.1 Introduction

A fundamental principle of Swedish and European legislation on processing of personal data is that personal data may only be transferred to a country outside the EU/EEA (a 'third country') if the receiving country has an "adequate level of protection" (33 § Swedish Personal Data Act). However, a number of exceptions are made from the requirement for an adequate level of protection, e.g. for transfers that are conducted in accordance with the standard clauses enacted by the EU Commission (34-35 §§ Swedish Personal Data Act). The Commission's standard clauses are issued in two main versions: for transfers between two data controllers ('*controller to controller'*-clauses) and for transfers between a data controller and a data processor ('*controller to processor'*-clauses).

As of 15th of May 2010, the Commission's *controller to processor*-clauses has been replaced by a new and updated set of clauses. This chapter 4 will highlight the most important changes in the new set of clauses and some of the issues surrounding the new standard clauses.

4.2 The New Standard Clauses

The previous set of *controller to processor*-clauses are and In this way, the registered individual is able to assert its rights to the same extent as would have been the case if the processing of personal data had taken place within the EU / EEA.

The new set of standard clauses was issued through Commission Decision 2010/87/EU, and replaces the older clauses as of the 15th of May 2010. The new set of clauses could be regarded as an update of the older clauses than a completely new regularization. They share the basic structure of the previous *controller-to-processor*-clauses[18], in the sense that they consist, somewhat simplified, of an agreement between a data controller within the EU / EEA (the exporter) and a data processor outside the EU / EEA (the importer). The rights and obligations of the parties under the agreement are subject to the law on data protection in the member state of the exporter, and the importer undertakes to process the data in accordance with "EU standard", i.e. in accordance with Data Protection Directive (95/46/EC).

18 The previous clauses were stipulated in the Commission Decision 2002/16/EC.

As a main rule, the new model clauses do not affect agreements concluded under the older set of clauses. Nevertheless, as soon as the prerequisites for the processing of personal data are changed, the new clauses are to be applied. Hence, the new clauses shall be applied as soon as any addition, re-negotiation or prolongation is made in connection with an agreement based on the older clauses.

The principal change brought by the new standard clauses is the introduction of a new subject. In addition to the signing parties (data controller and data processor) and the registered individual, a new subject, the *sub-processor*, is mentioned in the new set of standard clauses. A sub-processor is defined in clause 1 point d) as

> "any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract."

A sub-processor is thus a subcontractor of the processor, a contractor's contractor, who is assigned by the processor to handle all or parts of the personal data to be handled by the processor according to the processor's agreement with the controller. Since the definition does not only comprise a first-hand subcontractor but also a contractor of the processor's initial subcontractor, extensive chains of liability are rendered possible, in which multiple subjects could be considered as sub-processor(s) (provided that a number of requirements in clause 11 of the standard clauses are fulfilled). Through the requirement that processing of personal data in accordance with the new standard clauses may only be forwarded (to yet another party) on the original terms, the objective is for the new clauses is to ensure a European standard in all links of the chain. The older standard clauses could not be applied in the event that the processor intended to hire a sub-processor.

One reason for the introduction of the new subject sub-processor is probably because of lobbying from the IT industry, who strives to facilitate the transfer of production and delivery of IT services to more cost-efficient countries. This is related to the trends of *cloud computing* and *offshoring*, as described in Chapters 2 and 3 above. Transfer of personal data to third countries is often a prerequisite for successful and effective outsourcing projects that include offshoring and cloud computing.

Against this background it is however slightly disappointing that the Commission, when issuing the new set of standard clauses, has not catered for the situation in which a processor *within* the EU / EEA hires a sub-processor in a third country. The new standard clauses are only applicable in cases when a controller within the EU / EEA exports personal data to a processor in a third country. Hence, if a controller within the EU / EEA exports personal data to a processor *in another member state* and said processor transfers the personal data to a sub-processor in a third country, the new clauses are not to be applied (see

reason 23 of Decision 2010/87/EU). It should be noted that such a structure is not uncommon for cloud services.

The applicability of the clauses is thus restricted in a way which is unsatisfactory for the IT industry. For tax and organizational purposes, many global service providers have national units and entities within the EU, which are used as contracting parties in relation to the controller. A prerequisite in such outsourcing projects is however for the European processor to hire a sub-processor (or multiple sub-processors) outside the EU, either in the form of non-European companies within the same group of companies or through external partners. In this situation, the new standard clauses will not be applicable. In order to fulfill the legislation on personal data, the data controller must enter into an agreement also with the sub-processor.

Prior to the enactment of the new standard clauses, the consequence described above was observed by the Article 29-group, which a working group with the main objective of assuring that the Personal Data Directive is applied uniformly within the member states. The Article 29-group urged the Commission to immediately develop another instrument, aimed at the situation in which a European processor chooses to utilize a sub-processor in a third country. Until such an instrument had been drafted, the Article 29-group suggested that the Commission would urge the national authorities of member states to automatically accept all transfers from a European processor to a sub-processor in a third country, provided that such transfers are made in accordance with the new standard clauses.[19] In other words, if a processor within the EU / EEA was to hire a sub-processor outside the EU / EEA, these parties would, according to the suggestion of the Article 29-group, be able to utilize the new controller to processor-clauses analogously, with reference to the principles/motives of the new clauses, and thereby be deemed to fulfill the requirement on adequate protection for the rights of the registered individual.

4.3 Need for Additional Standard Clauses?

The Commission did not adhere to the recommendation put forward by the Article 29-group. The Commission stated in its decision that each member state should determine whether an agreement between a European processor and a sub-processor in a third country in analogy with the new standard clauses is to be deemed sufficient to fulfill the requirement that the rights of the registered individual are protected adequately.[20] As a consequence, the EU member states may come to have different views on whether, and if so to what extent, the new standard clauses can be applied analogously in connection with subcontracting-agreements. This causes an unfortunate lack of foreseeability that, in the opinion of the authors, means it is desirable for the Commission to introduce yet another set of standard clauses, this time in the form of *processor to processor*-clauses.

To summarize, the new standard clauses are likely to render the possibilities of transfer of personal data outside the EU / EEA more effective, in those situations where the data is to be processed by one or several sub-processors in

19 *See* p. 3 of Opinion 3/2009 of the Article 29-group.

20 *See* reason 23 in Decision 2010/87/EU.

the receiving country. In our opinion it is however regrettable that the Commission, when issuing the new set of standard clauses, did not clarify the rather common situation where a European data processor wishes to transfer personal data to a sub-processor in a third country. We therefore suggest that there is still a need for yet another set of standard clauses (*processor to processor*), in order to avoid complicated and impractical contractual arrangements between data controllers and sub-processors.

5 Recent Case Law Developments

5.1 The Pirate Bay

5.1.1 Introduction

One of the biggest problems for the software industry as well as other content providers has always been the threat of software piracy. In Sweden, 'file-sharing' has been made possible through various intermediaries over the years, such as Napster, Direct Connect and – perhaps most famously – *the Pirate Bay which* was launched in November 2003. The Pirate Bay website functioned as a search engine and provided so-called bit torrent files, which enables users to download copyright-protected material stored on other users' computers. At its peak, the Pirate Bay was immensely popular, having approximately 25 million users world-wide.

The Swedish police conducted a raid on the Pirate Bay servers in May 2006. In January 2008, prosecution under the Swedish Copyright Act (1960:729) was brought against the founders and co-funder behind the Pirate Bay on charges of 'contributory copyright infringement' for making available copyrighted works to the public. The court proceedings were initiated in the Stockholm District Court in February 2009.

5.1.2 Overview of the Legal Issues

5.1.2.1 The main offences

The main offences, i.e. the actual copyright infringements, were carried out by the users of the Pirate Bay when making available copyrighted works to the public. In the Pirate Bay case, the prosecutor claimed that the defendants, together and in mutual understanding, were *aiding* and *contributing to* these infringements by organizing, administrating, programming, financing and operating the Pirate Bay file sharing service.

Pursuant to the Swedish Copyright Act, a copyrighted work is communicated to the public when the work is made available to the public on the Internet through a wire or wireless connection from a place other than the place in which the public may review the work. This includes communication which takes place in such a manner that individuals may obtain access to the work from a place and at a time which they themselves determine, and thus comprehends the Pirate Bay file sharing service.[21]

21 *See* prop. 2004/05:110, p. 70.

5.1.2.2 Contributory Copyright Infringement

The legal concept of contributory liability, i.e. to physically or psychologically facilitate the commission of a crime, is sanctioned under the Swedish Penal Code. The contributory act does not need to have been a prerequisite for the realization of the main offence. Furthermore it is not, in the District Court's opinion, required that the person committing the main offence is identified in order for contributory liability to arise.

In addition, the defendants must have intentionally contributed to copyright infringement in order to be held liable. This requirement must be fulfilled with regard to the actual contribution as well as with regard to the main offence. In its ruling, the District Court held that it is sufficient that the defendants intended that copyright protected works as such were made available in order for the requirement to be fulfilled.

5.1.2.3 Joint Criminal Liability

Joint liability presumes that each individual has participated in the offence and was aware of the actions of the others. Since the defendants all had direct or indirect influence over the Pirate Bay file sharing service, and since the defendants acted and functioned as a team, the District Court held that all defendants were liable jointly.

5.1.2.4 Discharge from Liability

According to the District Court, the Pirate Bay is to be regarded as a service provider that provides a service at a distance, by means of electronic equipment for processing, and at the individual request of the users.[22]

Under Article 14 of the E-Commerce Directive, liability is under certain circumstances exempted for service providers that store information provided by a service recipient. In the opinion of the District Court, services that provide server space where users can upload and store torrent files on a website fall under this Article. The service provider is exempted from liability either if (i) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or (ii) if the provider, upon obtaining such knowledge or awareness, acts swiftly to remove or to disable access to the information.

Since the defendants were aware that torrent files which indicated protected works were available on the Pirate Bay website, and that none of them took any measures to remove these files (regardless of several requests to do so), the defendants were not exempted from liability.

5.1.2.5 Damages

In connection with the criminal case against the founders and co-funder of the Pirate Bay, individual civil compensation claims in a total amount of approximately EUR 13 million were filed by a number of right holders,

22 Article 2 in the Directive 2000/31/EC on Electronic Commerce.

including Nordic film companies, American film companies and Swedish record companies.

Pursuant to the Swedish Copyright Act, the right holder is entitled to reasonable compensation for unlawful use of copyright protected works, regardless of whether the right holder suffers any prejudice from the use. Compensation shall also be paid for further damage caused by the infringement, provided that the unlawful use is willful or with negligence. The damages shall fully cover the loss incurred.

In their claims, the right holders used different models for calculation of *reasonable compensation* and *further damage*. When determining the reasonable compensation, the District Court held that it is customary for damages to be based on tariffs, collective agreements or similar, or from fundamental rules and conditions in the industry or market on which the use took place, in order to establish a hypothetical licensing fee for the use. If such guidance is not available, the court ultimately assesses the reasonable compensation. In addition, the right holders claimed further damages in the form of sales losses, market damage, certain internal losses, and loss of goodwill.

The District Court awarded the Nordic film companies reasonable compensation in accordance with their claims, which amounted to between EUR 15,500 to EUR 72,500 for each film that had been made available. The American film companies and the Swedish record companies were awarded compensation equivalent to half of the number of downloads claimed. The District Court estimated the further damages to half the amount of the reasonable compensation.

5.1.3 The Ruling

The District Court rendered its judgment in April 2009, sentencing each of the four defendants to one year's imprisonment. The District Court further awarded the right holders damages amounting to approximately EUR 3.3 million.

The defendants have appealed the judgment to Svea Court of Appeal. The main proceedings are scheduled to begin on the 28 September 2010.

It is likely that the case will be granted leave for appeal to the Swedish Supreme Court, due to the lack of existing case law with regard to contributory copyright infringement in Sweden.

5.1.4 Implications of the Pirate Bay Case

As the case is still subject to an appeal, it is not yet possible to fully analyse the implications of the Pirate Bay case. It is clear that 'file sharing' services such as the Pirate Bay will continue to be replaced by new Internet services such as Spotify and Voddler, through which copyrighted content can be accessed legally at little or no cost for the user.

It should also be noted that several other civil proceedings have been initiated in Sweden with regard to Internet service providers that provide Internet access to the Pirate Bay website. Notable examples include IFPI v. Black Internet AB and MPA vs. Portlane.

Another interesting development in the work against piracy over Internet is the possibility to gain access to information on the owner of IP-adresses set out by the EU Enforcement Directive. This is starting to be used by rightholders, but

the legislation is circumvented by tools to make the IP-adress anonymized, Pirate Bay has for example as a first page an application with this purpose to download.

5.2 Google AdWords

In addition to the Pirate Bay case, another important ruling regarding liability for online intermediaries was made in the spring of 2010 by the European Court of Justice (ECJ) in a case between Google and Louis Vuitton regarding 'Google AdWords'.[23] The essential legal issue was the interpretation of Article 14 of the E-Commerce Directive (see section 5.1.2.4 above).

Google AdWords is an advertisement system operated by Google, which allows advertisers to place advertising links to the advertiser's website on the side of Google search engine. The advertisers select keywords which respond to the entry of those keywords in Google search engine.

In its ruling, the ECJ held that Google AdWords should be considered as an information society service, since the service is provided at a distance, by electronic means and upon the individual and explicit request of the advertisers. Even if Google search engine is provided free of charge, it is provided in the expectation of remuneration under AdWords.

The assessment whether a service provider may be exempted from liability under Article 14 of the E-Commerce Directive is in the ECJ's opinion dependant on the role played by the relevant service provider. In this regard it is important to determine whether the service provider's conduct has been merely technical, automatic and passive, i.e. if the provider lacks of knowledge or control of the stored data.

In ECJ's opinion, Google was exempted from liability under Article 14 since Google had no knowledge of, or control over, the data stored on its servers. The ECJ held that the assessment whether a service provider in such a scenario shall be exempted from liability under Article 14 of the E-Commerce Directive, shall be determined by national courts.

Although the aforementioned cases concern trademark infringements, it is likely that the principles set by the ECJ would be applied similarly to intermediaries which are involved in copyright infringement.

5.3 Personal Data on Facebook and Other Social Media

5.3.1 Introduction

User-generated content on social media, such as comments, announcements, blogs and clips, is uploaded and distributed between users instantly. Such content will often include personal data, which means that data protection laws are applicable and must be considered in relation to such content. In fact, it is generally considered that online processing of personal data on social media represents a significant challenge to the legal framework for data protection in Sweden and abroad, since the pace at which such data is processed is both extremely rapid and ever-growing.

23 GoogleFrance v. Louis Vuitton (and others) in the joined cases no C-236/08, C-237-08 and C-238/08.

As already mentioned above, the Swedish Personal Data Act (1998:204) is designed after the Data Protection Directive (95/46/EC) and is thus based on certain subjects to be identified when processing personal data. By distinguishing a 'data controller' (he who alone or jointly determines the means of the processing of personal data), a 'data processor' (he who processes personal data on behalf of the controller) and a 'data subject' (he whom personal data relates to), the Personal Data Act strives to achieve a clear-cut assignment of responsibility between the different roles. Somewhat simplified, the processor is in control of and has responsibility over the data, whereas the data processor only handles the data in accordance with the controller's express instructions.

Such a traditional view on the different roles of data processing is not always easy to apply on the interactive and multi-contributory environment of social media. For example, the social network service *Facebook* allows a user to create and customize his or her profile, which may be viewed and altered by other users, for example by other users leaving a "post" on the profile "wall". The configuration and operation of the service, (including the choice of which marketing is to be allowed on the site etc), is however made by the service provider itself, i.e. Facebook.

In this situation, the roles prescribed in the Personal Data Act for determining the identity of the data controller, data processor and data subject are not easily applied. Does, for example, the fact that the service provider decides the technological framework for the processing make the provider a controller, even though it has no reasonable chance of surveying the data processing of every profile holder? And *if* the service provider is to be regarded as the controller, should the profile holders be considered as data subjects, processors, or "co-controllers", considering the fact they are in fact able to process other users' personal data by way of their profiles?

5.3.2 Recent Decisions by the Swedish Data Inspection Board

During the spring of 2010, the Swedish supervisory authority the Data Inspection Board initiated a project with regard to the use of social media by Swedish authorities, municipalities and corporations, by carrying out inspections of one Swedish authority (*Arbetsmiljöverket*), one Swedish municipality (*Katrineholms kommun*) and one Swedish corporation (*Gröna Lunds Tivoli AB*).[24] All three organizations used Facebook, and Katrineholms kommun also had its own blog as well as a *Twitter* page. The results of this project were published in July 2010 in form of three decisions by the board.[25]

According to the decisions by the Data Inspection Board, a profile holder on Facebook should be regarded as the data controller of *all* personal data processed on its profile, irrespective of whether the data is posted by the holder itself or by other users. The board came to the same conclusion with regard to blogs, but not for the use of the social network service Twitter. On Twitter, the profile holder is the data controller in relation only to such personal data which is posted by the profile holder.

24 Press release 2010-04-12 *"Datainspektionen granskar användningen av sociala medier"*.

25 Decisions 685-2010; 686-2010 and 687-2010.

The reasons for the decision are that the profile holder is the subject who (i) chooses to be present on the social media, (ii) names the profile page, (iii) determines the possibilities for other users to post content on the page, (iv) determines the overall content on the page and (v) has the authority to delete specific posts or the entire page. Another important aspect is that all posts on the page would be permanently deleted if the profile holder would decide to close the page. As a consequence, the board considered that the profile holder is the person who decides "the purpose and means of processing personal data" (3 § Personal Data Act), i.e. the profile holder is the data controller for all personal data on the page.

Further, the Data Inspection Board considered – due to the frequent use of Facebook in the ordinary course of life and with respect to freedom of information and free speech – that personal data on Facebook was *not* structured in a way that "significantly simplifies searching or compilation of personal data". This means that a specific exception to several rules in the Personal Data Act is applicable (5a § Personal Data Act), and that processing of personal data on social media is allowed provided that the personal integrity of the data subject is not violated.

According to the decisions made by the Data Inspection Board, the consequences of carrying the role as a data controller for personal data on social media essentially involves a responsibility to ensure that all processing is made in accordance with the Personal Data Act. This includes (i) a responsibility to ensure that processing of data which may violate the personal integrity of the data subject does not occur (and to remove any such violating personal data once discovered), (ii) to compensate any data subject whose personal data is processed incorrectly, and (iii) to ensure that any person working with the social media only does so in accordance with the controller's instructions. In addition, the data controller must take appropriate technical and organizational measures to protect the processed data. Taking into account the limited level of influence on security measures that a profile holder has on Facebook, the Data Inspection Board however affirmed that this responsibility "rather tends to be of organizational than of technical nature".

The scope and purpose of a profile page could affect which security measures are taken. If there is an apparent risk for sensitive information to be posted on the page, e.g. information regarding ethnicity or political conviction, more far-reaching measures will need to be taken. Further, the profile holder is also responsible to take appropriate precautions to ensure that the processing of personal data is compliant with the Personal Data Act. Such measures could include publishing user instructions regarding the purpose of the page, for which purposes users may post content on the page, what type of posts that are not allowed and the consequences of non-compliance with such instructions.

With regard to the obligation of the profile holder to remove personal data which violates personal integrity, the board states that such responsibility arises as soon as the profile holder becomes aware of such information. The determination of what constitutes a violation of personal integrity must be made on a case-by-case basis taking into account the context in which the data is processed, for what purpose it is processed and the dissemination (including the possible risk for dissemination) of the data. In its decisions, the Data Inspection

Board specifically emphasizes that the risk for dissemination and violation of personal integrity will increase if the data is made available to indexation by search engines.

The decisions by the Data Inspection Board gives rise to several questions. First of all, it is slightly surprising that the board has made such clear statements regarding the responsibility for personal data on social media, since these decisions have not been made in a legal vacuum. For example, it would have been very interesting to learn how the Data Inspection Board interprets the relationship between these decisions and other legislation regarding online intermediaries.[26]

Secondly, the Data Inspection Board's decision to deem profile holders responsible for all posts on its blog or social network profile pages does not address the situation where individuals use "professional" profile pages on social media for private purposes, or when employees create profiles or blogs which are related its employer without such site being actually or consciously administered by the employer (e.g. the social service *LinkedIn*). In such cases, it could perhaps be questioned whether the decisions of the Data Inspection Board could come into conflict with 6 § Personal Data Act, according to which data processing by physical persons of a private nature is exempted from the Personal Data Act.

Last but not least, it could be questioned to what extent the so-called hosting defense under Article 14 of the E-commerce Directive[27] applies in relation to social media (see section 5.1.2.4 above). Subjects such as online newspapers[28] and online search engines[29] have successfully relied upon Article 14, and in our opinion it is not unfeasible that authorities, municipalities or corporations could rely on similar defenses with regard to the use of blogs, social networks and similar media.

26 In this respect the E-commerce Act (2002:562) and the Act on Responsibility for Electronic Notice Boards (1998:112) is of particular interest.

27 European Directive on electronic commerce (2000/31/EC).

28 Karim v Newsquest Media Group (27 October 2009) English High Court (Eady J).

29 GoogleFrance v. Louis Vuitton (and others) in the joined cases no C-236/08, C-237-08 and C-238/08.