CLOUD COMPUTING IN POLAND

REGULATORY FRAMEWORK

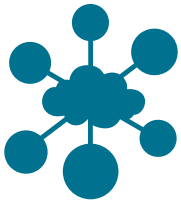


TABLE OF **CONTENT**

FOREWORD

We are pleased to introduce to you this Cloud Computing in Poland – Regulatory Framework.

This publication addresses the most important legal issues relevant for legal practitioners and business people dealing with cloud computing products and services in Poland.

This survey was prepared and coordinated by the specialist cloud computing and data protection team at PIERSTONE, a technology law firm in Prague, Czech Republic.

The article Cloud Computing – Brief Technical Overview for Legal Professionals was written by Zdeněk Jiříček, freelance cloud consultant based in Prague, Czech Republic.

We would like to thank Dr. Jochen Engelhardt, CEE Legal Director, Legal and Corporate Affairs at Microsoft who proposed the idea for this publication and supported its realization.

Editors: Lenka Suchánková, Partner (lenka.suchankova@pierstone.com), and Jana Pattynová, Partner (jana.pattynova@pierstone.com), PIERSTONE.

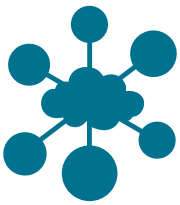
HOW TO USE THIS PUBLICATION

This publication consists of four parts.

The first part of the survey consists of two articles addressing the concept of cloud computing from both a technical and a legal perspective; it is complemented by a definition section outlining the main terminology used in the Q&A section of the publication. These introductory chapters are followed by a general overview of EU personal data protection legislation relevant to cloud computing, presented in a Q&A format. The last part of the publication contains a country-specific questionnaire describing key data protection requirements relevant to cloud computing under Polish law.

The aim of the country-specific Q&A is to highlight areas that diverge significantly from the general EU-wide data protection regulation and as such, shall always be read in connection with the general overview of EU personal data protection legislation which serves as a point of reference.

Disclaimer:This publication is for informational purposes only. The information contained in this publication is intended only as general guidance on selected data protection aspects of cloud computing. It does not deal with every relevant topic or may not address every aspect of the topics covered. This publication may be updated from time to time. The application and impact of laws may vary widely based on the specific facts involved. The information does not constitute professional legal advice and should not be used as a substitute for consultation with a legal adviser. Before making any decision or taking any action requiring legal assessment, you are advised to consult a legal professional.



TERMS USED IN THE QUESTIONNAIRE SECTIONS

Cloud Opinion	Opinion 05/2012 on cloud computing released by the EU Article 29 Working Party (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).
Draft EU Data Protection Regulation	Draft proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) of 16 January 2013 (http://www.europarl.europa.eu/document/activities/cont/201305/20130508ATT65784/20130508ATT65784EN.pdf).
DPA	Data Protection Authority.
EEA	European Economic Area.
EU Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT).
EU Standard Contractual Clauses	European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF).
EU-US Safe Harbor Framework	European Commission Decision of 6 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML).
Personal data	as defined in Art. 2 (a) of the EU Data Protection Directive.
WP 29	The Data Protection Working Party established by Article 29 of the EU Data Protection Directive.

CLOUD COMPUTING – BRIEF TECHNICAL OVERVIEW FOR LEGAL PROFESSIONALS

Zdenek Jiricek, *Freelance cloud consultant, Prague, Czech Republic*

INTRODUCTION

Cloud computing represents a huge paradigm shift in the way that computing power is provided to organizations and to end users. Organizations can now choose – instead of procuring their own hardware and software licenses - which parts or layers of the computing architecture to own, and which to rent, and on what terms and conditions.

The simplest parallel that comes to mind is the one related to supply of electrical energy. About two hundred years ago, during the transition from the first to the second industrial revolution, factories used to rely on their own steam power generators. It was only later on when the mass production of electricity won on costs and reliability over the individually operated power supplies. The energy market developed into a regulated industry driven by competing power companies offering different pricing schemes for energy, typically separated from operation of the power grid. It seems to be economical to trade spikes of power across national borders, even in spite of some technical difficulties related to interoperability (the need for so-called phase convertors).

Similarly, computing power may be offered more economically and with higher flexibility through a level playing field of providers offering computing services out of their „cloud“ infrastructures, typically through Internet connectivity. The potential benefits of cloud computing are enormous. They include greater efficiencies for organizations to customize and rapidly scale their IT systems for their particular needs, expanded access to computational capabilities previously available only to the very largest global companies, better collaboration through “anywhere, anytime” access to IT for users located around the world, and new opportunities for innovation as developers flock to this latest computing paradigm. For governments in particular, cloud computing offers the potential to reduce costs in a time of economic constraints while making data more easily accessible to citizens and making the process of governance more transparent.

CORE ATTRIBUTES OF CLOUD COMPUTING

According to NIST[1], cloud computing is a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort" of the cloud service provider. It has 5 essential characteristics:

- **On-demand self-service:** a client administrator can provision computing capabilities automatically, without requiring human interaction with the service provider.
- **Broad network access:** variety of client platforms (PCs, tablets, smartphones) may access the computing capabilities over the network.
- **Resource pooling:** the cloud service provider's resources are pooled to serve multiple consumers using a multi-tenant model, when different physical and virtual resources are dynamically assigned according to consumer demand.
- **Rapid elasticity:** capabilities can scale rapidly up and down so they appear to be unlimited to the consumer, and to be available at any time.
- **Measured service:** resource usage has metering capability while providing transparency for both the provider and consumer of the utilized service.

CLOUD DEPLOYMENT MODELS

There are two primary criteria used to classify the various deployment models for cloud computing: Location of where the service is running (premise of the customer or the data center of the cloud service provider) and level of access (shared or dedicated to a single organization).

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization or enterprise comprising multiple user groups (e.g., business units). It may be owned, managed, and operated by the organization or by a third party. If the dedicated resources are hosted, it may be considered a special type of private cloud called "Hosted Private Cloud". Examples: IT who could run HR, Finance, Accounting, and Business Process Applications on the same on-premises, fully virtualized shared infrastructure, provided to multiple business units of the same organization.

1 U.S. National Institute of Standards and Technology - The NIST Definition of Cloud Computing, Sept. 2011
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- **Public cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Resources are externally hosted and are dynamically provisioned and typically billed according to a structured price list. Examples: Microsoft Office 365, Amazon EC2, Microsoft Azure Platform, Salesforce.com, Google Apps.
- **Hybrid cloud.** The cloud infrastructure is a composition of private and public clouds that are usually provided through separate arrangements, but are bound together for data and application portability. Example: public cloud providing offloading capability for specific workloads.

CLOUD SERVICE MODELS

Depending on user requirements, there are several cloud computing solutions available on the market; they can be grouped into three main categories or "service models". These models usually apply to both private and public cloud solutions:

- **Infrastructure as a Service (IaaS):** a cloud provider leases virtual remote servers that end users can rely on in accordance with provisioning mechanisms and contractual arrangements. This model is comparable to a situation when customers install both the operating system and the applications on new hardware themselves, and they are responsible for keeping the whole software stack up to date and manageable. The real difference is that in the case of cloud IaaS this "new hardware" is not physically available locally, but it's available "somewhere in the cloud" in the form of a "virtual computer" or "virtual machine" through Internet connectivity. Customers usually install so-called "images" of the complete software stack into such a remote virtual server environment. The terms and conditions usually include metered-by-use cost model and allow the end user to expand their use of the infrastructure as needed, usually via self-service portals. Examples include: Microsoft Azure Virtual Machines, Amazon EC2, Hosting.com, private clouds deployed/ managed by IT as service to business units.
- **Platform as a Service (PaaS):** a cloud provider offers solutions for hosting of applications. As a simplified description, the customer gets a virtual computer (or "virtual machine") in the cloud running a particular type and version of the operating system, together with needed middleware and libraries that support installation of compatible applications. The comparison here is to installing an ERP enterprise software on a remote server with preinstalled Windows Server or Linux operating system. The cloud provider is responsible for keeping the operating system up to date, and for managing all the underlying hardware and networking. PaaS is widely used for testing and deployment of new applications without having to provision local virtual machines together with instances of the operating system. Examples include: Microsoft Azure Platform, Google App Engine, CloudFoundry.org.
- **Software as a Service (SaaS)** is a model where an application is delivered over the Internet and customers pay on a per-use basis. In SaaS, the

customer is only focused on the finished application, without having to manage the application or the underlying operating system and infrastructure. It is the most common form of cloud computing delivered today. Examples include: Microsoft Office 365, Salesforce.com, Hosted Exchange.

KEY ADVANTAGES

From an overall perspective, cloud computing offers the following advantages:

Lowering barrier of entry to global markets for Small and Medium Enterprises ("SMEs"). SMEs don't have to worry about high initial investment costs related to procurement of the needed hardware, software and system administration services to operate their own advanced server infrastructures. They can quickly subscribe to and start consuming "IT as a service" acquired "on demand" from a cloud service provider. This way SME's can improve their business agility and innovate through employing state-of-the-art information infrastructure, previously available only to large enterprises, and become much more competitive in their global supply chains.

Reducing Total Cost of Ownership in comparison to operating own ICT infrastructure. There are multiple efficiency aspects acting in synergy in favor of cloud computing: from increased physical utilization of servers, through flexible reallocation of computing resources to a variety of customers, up to high level of automation provided to system administrators – that all contribute to a reduction in cost per transaction or cost per managed server. And further on, software vendors may achieve higher efficiency by employing multi-tenancy on application level – meaning that commodity applications may be launched in a virtual machine only once, and still made available to tens or hundreds of simultaneously connected cloud customers (typically SME's), in virtually separated areas. The below graph is based on Microsoft's public cloud operating cost estimates and suggests that total cost of ownership ("TCO") per managed server of large public cloud infrastructure compared to server infrastructure of SME is 40 times lower, or approx. 10 times lower compared to TCO efficiency of a large private cloud:

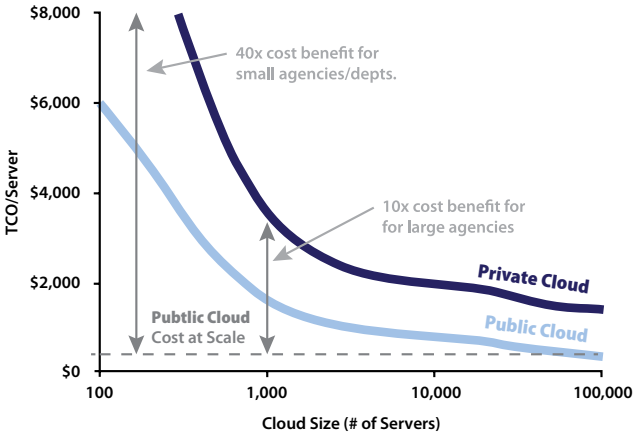


Figure 1: Cost per managed server – Small enterprise, Private, Public clouds[2]

2 Microsoft Corp.: The Economics of the Cloud For the EU Public Sector (2010), page 17
http://www.microsoft.com/global/eu/RichMedia/eu_public_sector_cloud_economics_a4.pdf

Anyone may become a global software supplier. Software start-ups and local Independent Software Vendors may become global suppliers through PaaS or SaaS solution offerings - so called "micro-globals" of the 21st century. Anyone can sell their software through the various cloud application markets – either as SaaS (e.g. Microsoft Azure Marketplace, Salesforce AppExchange, NEC Cloud Marketplace), or as licenses through mobile application markets, which is also a form of cloud service (e.g. Windows Store, Apple iOS App Store, or Google Play).

Enabling mobility and flexible working. Through its ubiquitous presence and its ability to support a variety of client devices and platforms, cloud services become an ideal back-end for all PCs, tablets, smartphones, and perhaps wearable or embedded devices of the future. Software-as-a-Service applications sourced to thousands of customers have to be fast in supporting multiple client platforms, as requested by the diversity of their SaaS customers. Email, calendaring, or video conferencing in the form of cloud SaaS will be easier to connect to from home or other remote places, while employing Bring-Your-Own-Device strategies. The overall level of service assurance of the leading cloud service providers is generally higher than the one that SME's can afford, especially when it comes to 24x7 availability and service continuity.

Business continuity and Operational resilience. Cloud providers typically offer 99.9% Service Level Agreements, sometimes supported by a money-back guarantee. Microsoft's Office 365 average availability was 99.96% in the year 2013 (as published on Office 365 Trust Center[3]). Customer data are normally stored on 3 independent hard drives in each data center, and many cloud services provide automatic versioning of saved documents. Customers may opt for geographical redundancy and have their data synchronized to another remote datacenter, which further improves business continuity.

Protection against cyber threats. Renowned cloud providers may become an easy target to "Denial of Service" type of attacks. On the other hand, cloud providers typically operate 24x7 supervision centers that can quickly alert customers of cyber-attacks and they have a broad set of tools on hand such as scaling out capacity, packet filtering, and traffic throttling in order to keep the cloud services at high availability level. Also, cloud providers have vastly improved anti-malware and spam filtering at the entry point of their email, calendaring, and document collaboration services, using the latest network analysis technologies and nearly real-time malware signature updates.

3 Office 365 Trust Center: http://trustoffice365.com/; Look for title "Office 365 availability"

TECHNICAL CHALLENGES AND POSSIBLE SOLUTIONS

Apart from legal compliance issues that are the subject matter of this booklet, let's take a look at the biggest cloud architectural and operational challenges:

Security vs. Multi-tenancy. The cloud efficiency gains may be achieved primarily through effective resource pooling and sharing; this means that cloud providers aim at high levels of multi-tenancy, ideally up to sharing the same software program instance among multiple customers. Hence it is important to securely virtualize the application environment for every customer, isolate their data, and possibly create secure "sandboxes" where custom code may be executed within shared SaaS services such as Office 365.

Integrated system administration. Few customers will migrate all of their IT systems to the cloud in the foreseeable future. Most customers will think in terms "which cloud model is right for me", and "which apps should we migrate to the cloud first". Routine operations that system administrators do repetitively, such as creating a new user account or scaling up/down their virtual machines, should be achieved with high levels of automation. Ideally, the same system administration tools should be capable of managing both on-premise datacenter as well as cloud virtual resources.

Secure and Single Sign-on Access. Having in mind the ubiquitous presence of online services and global cloud accessibility over the Internet, the question comes to mind "how do we manage secure access to cloud services for our active employees all the time". This includes tasks such as enforcing strong log-in credentials in the cloud, managing real-time authorization for the employees – especially as they join and leave the organization - and ideally achieving true single sign-on to both local and cloud-based services. That assumes dynamic verification of the employee's status in the home directory performed in such a way that there is no noticeable difference between accessing on-premise or cloud based applications, for employees working from the office, but also working remotely.

Encryption and Key management. The cloud provider is typically responsible for encryption of customer data during transfers (i) from client devices to the cloud and back, (ii) while synchronizing backups between datacenters, and (iii) storing data in the physical hard drives in the cloud. This, together with other organizational security controls, should provide high degree of assurance that customer data will not be misused. However, in case of processing sensitive data in the cloud, customers may require an additional layer of encryption that would completely eliminate access to the customer data in open form, while in the cloud infrastructure. This brings new functionality challenges to processing encrypted customer data by cloud services such as document search or business intelligence, which may be limited or require alternative approaches.

Software version and change management. One of the key advantages of cloud PaaS and SaaS services is that "someone else" (i.e. the cloud provider) takes

care of keeping the software patched, up to date, and deploying new capabilities (software upgrades). That may raise new kinds of concerns to the customers: are we ready to consume the new versions at the pace scheduled by the cloud provider? Will our users be ready and trained for it? Shall we experience integration issues with other systems? It makes sense to verify with the cloud provider how much the customer may influence the schedule of upgrades on the services coming from the cloud.

CLOUD ADOPTION OUTLOOK

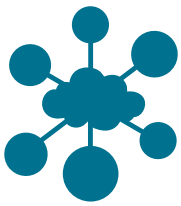
According to IDC research from Dec. 2013[4], the fastest growing segment of cloud services globally will be SaaS - it is predicted to grow nearly five times faster than the software market as a whole. By 2016, nearly $1 of every $6 spent on packaged software, and $1 of every $5 spent on applications, will be consumed via the SaaS model. By 2016, about 25% of all new business software purchases will be of service-enabled software, and SaaS delivery will constitute about 16.4% of worldwide software spending across all primary markets and 18.8% of applications spending.

Cloud computing is one of the current "megatrends" – together with mobility, social, and BI/big data. A study by Ipsos MORI[5] shows that cloud adoption in EMEA region may be fastest among SME's, with 53% of the 6,800 surveyed companies already using cloud computing for at least one of the listed services - which were email, data storage, document exchange, instant messaging, voice over IP, productivity suites, video conferencing, and processing power (ordered by frequency of response). 28% of them said that their organization was likely to shift more spending towards cloud solutions over the coming year. And most importantly, 74% of those already using cloud computing were positive about how well their IT solutions help get their job done, vs. 61% of those not using cloud computing. The SME's using cloud were also more confident about their business prospects (33%) than those not using it (26%), and they were more often planning to launch new products or services, expand into new markets, and invest into efficiency or productivity gains.

In general, the biggest cloud opportunities perceived by business management are (i) IT efficiency – deliver IT resources quickly and at an acceptable price point, (ii) IT agility – services that are easily consumable, consistent, and paid-per-use, and (iii) Business innovation – cloud helps address customer opportunities faster, enable and optimize business performance. Cloud services embraced first by customers usually replace commodity on premise software (e.g., email, collaboration, calendaring, and voice/video conferencing), data backup and archiving, and most recently also business processes such as CRM, payroll, procurement, and other web applications.

4 IDC Market Analysis Perspective: Worldwide SaaS and Cloud Software, 2013 (IDC #245047) http://www.idc.com/getdoc.jsp?containerId=245047

5 Ipsos MORI SMBs and Cloud Computing EMEA study (2013) http://download.microsoft.com/download/3/5/2/35261139-417E-43B1-84A6-663646881E11/Microsoft%20EMEA%20SMB%20Cloud%20Survey%202013.pdf



CLOUD COMPUTING AND **DATA PRIVACY**

Mgr. Jana Pattynová, LL.M., *Partner, PIERSTONE*
Mgr. Lenka Suchánková, LL.M., *Partner, PIERSTONE*

From being perceived mainly as a marketing catch phrase, cloud computing has evolved into an increasingly commonplace tool which an ever-growing number of information technology users rely on, whether knowingly or not, on a daily basis. From a technical perspective and in a nutshell, cloud computing can be characterized as a service which allows its users an easy access to configurable IT services such as networks, servers, data storage or applications and programs through the internet; data or programs can be stored on external servers instead of on the user's computer, often located thousands of kilometers away from the user. In this context, the remote server is usually depicted as a "cloud" – hence the term cloud computing.

From European law perspective, cloud computing is, in line with *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society*, considered a service rather than a software concept. One important implication of this perception is that, compared to the more traditional licensing models, the doctrine of exhaustion of rights would not apply to the provision of ICT services through cloud. EU law offers neither a legal definition nor any comprehensive legal framework for cloud computing but it has become obvious that, at least in the EU context, the major legal concerns surrounding cloud computing arise in the area of data protection and security, notably the protection of personal data. This article offers a view on selected legal aspects of cloud computing through the prism of EU legislation governing personal data protection in general, with a small detour to sector-specific regulation.

PERSONAL DATA AND THE CLOUD – WHO ARE THE KEY PLAYERS

It is now generally accepted that cloud computing services, whether provided as a SaaS, PaaS or IaaS service model, will involve some kind of processing of personal data. Cloud computing scenarios involve a range of different players and, from the perspective of EU data protection rules, cloud solution providers will usually be considered 'data processors' while cloud customers who determine the ultimate purpose of the processing and decide on the outsourcing and the delegation of all or part of the processing activities to an external organization will in most cases be deemed 'data controllers'. This rule, however, is not

unconditional and the determination of roles of the key stakeholders will largely depend on the specific circumstances of the case. For example, where a cloud provider processes the entrusted personal data for its own purposes, it may attain the status of a joint controller or even a controller in its own right.

The rules on allocation of responsibilities between these two parties, elaborated on by the Article 29 Data Protection Working Party in its Opinion 05/2012 on cloud computing from 1 July 2012 (the "Cloud Opinion") make it clear that it is the primary responsibility of the personal data controller – i.e., the cloud customer - to guarantee, at any time, a high standard of security of the personal data that it entrusts to a cloud provider for processing. The cloud customer should therefore conduct an in-depth analysis of the potential risks associated with the use of cloud-based solutions and arrange for appropriate technical and security measures as well as sound contractual safeguards (including those that ensure the lawfulness of any cross-border personal data transfers) prior to deploying a third party cloud solution.

DATA PROCESSING AGREEMENT

One of the key pillars of data processing in the cloud is a written agreement (or an agreement concluded in "another equivalent form") on the processing of personal data ("data processing agreement"). A data processing agreement needs to be executed between the data controller and the data processor before any data processing operation in the cloud is carried out. At the very minimum, such agreement must stipulate that the data processor may only act on the instructions from the data controller and it should provide guarantees of the data processor with respect to the technical and organizational security measures implemented to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing. EU Member States may and usually do prescribe further requirements for data processing agreements, such as the specification of personal data being processed and the scope of processing, the purpose and period of processing, or allocation of responsibilities between the contracting parties.

MULTIPLICITY OF PROCESSORS

Cloud computing services frequently entail the involvement of a number of contracting parties who act as processors, or sub-processors of the original data processor. Such sub-processing is generally permissible provided, however, that the processor makes this information available to the cloud customer, disclosing details about the type of service subcontracted, the characteristics of current

or potential sub-contractors and provides guarantees that these entities undertake to comply with the relevant data processing law implementing the EU Data Protection Directive; a flow down of the relevant data processor's obligation under its contract with the cloud customer to the sub-processors through appropriate contracts must be ensured.

IF A CLOUD PROVIDER IS LOCATED ABROAD

The intrinsically global nature of cloud computing services means that the data centers where users' data are stored are often located outside of the country where the cloud customer is located. As a result, the use of cloud computing services frequently entails cross-border flows of personal data which in turn requires that the parties pay an increased attention to the appropriate data transfer regime.

Rules for cross-border data transfers vary depending on to which country personal data are exported. Personal data transfers within the borders of the EU and EEA cannot be restricted in any way and personal data may thus be transferred freely without any limitations (as long as other legal requirements pertinent to data processing are met, such as the existence of a proper data processing agreement providing for adequate technical and organization security measures). The same rule applies to data transfers to countries that are a party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, ETS 108, 1981). Similarly, unrestricted transfer of personal data is permitted to countries explicitly "white-listed" by the decisions of the European Commission (such as, by way of examples, Argentina, Israel, or New Zealand).

By contrast, transfers of personal data to third countries which do not offer an adequate level of data protection require specific safeguards such as the use of the EU-US Safe Harbor arrangements, EU Standard Contractual Clauses or Binding Corporate Rules (BCR), as may be appropriate in the individual cases. European Commission Decision of 6 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (the "EU-US Safe Harbor Framework") which covers the specific case of personal data transfers to Safe Harbor-certified entities in the United States has recently come under mounting criticism from EU institutions and leading individuals, including, in particular, Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship. As calls for its suspension abound and the first revision of this Euro-Atlantic contractual framework is scheduled in summer of 2014, European cloud customers relying on the EU-US Safe Harbor Framework for data transfers to the United States should monitor the developments closely and may be compelled in the future to explore alternatives that would guarantee lawfulness of personal data transfers across the Atlantic.

For the time being, the key alternative mechanism for cross-border data transfers to third countries which do not offer a level of personal data protection

corresponding to the EU level, are undoubtedly the so called EU Standard Contractual Clauses[1]. In the view of the Article 29 Data Protection Working Party, sole self-certification with the EU-US Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment; by contrast, the EU Standard Contractual Clauses are generally deemed to offer a robust protection for customers transferring personal data to third countries. This is why the Article 29 Data Protection Working Party encourages European data exporters to use this legal instrument (in addition to BCR which use, however, is restricted to intra-group transfers and as such is of limited relevance for cloud transfers). While in many EU Member States the deployment of the EU Standard Contractual Clauses is considered to adduce sufficient data protection safeguards and their use in an unmodified form does not require any further regulatory approvals, the laws of some EU countries nevertheless still require some form of approval by or notification to the national Data Protection Authority prior to their deployment.

PRINCIPLES UNDERPINNING A CLOUD AGREEMENT

The Cloud Opinion stresses that the lawfulness of personal data processing in the cloud strongly depends on the adherence to basic principles that underpin EU data protection law, namely transparency vis-à-vis the data subject, the principle of purpose specification and limitation, and the adequacy of contractual safeguards implemented to ensure data protection and data security. These principles can be summarized as follows:

- **Transparency** The user of cloud services should always be informed of all important aspects of personal data protection, in particular of any potential subcontractors involved in the processing, places where data may be stored or processed or technical and organizational measures of the provider.

- **Purpose specification and limitation** Restrictive contractual arrangements (such as an explicit prohibition for the cloud provider to use customer's data for advertising purposes) and contractual treatment of data deletion after cessation of the purpose of their processing and particularly after termination of the agreement should be incorporated into a cloud contract. An explicit stipulation in the agreement that the ownership rights to the data does not pass onto the cloud provider is highly advisable.

- **General contractual safeguards** A cloud contract should specify the security measures that the cloud provider must comply with as well as

1 European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

details on the extent and modalities of the cloud customer's instructions to be issued to the cloud provider, including service levels, and relevant sanctions for non-compliance with service levels (which usually have the form of either contractual penalties tied to a breach of service levels, or are modeled along service credits and discounts).

- **Contractual safeguards regarding access to data** Only explicitly authorized persons bound by confidentiality obligations should be allowed access to data stored in the cloud.

In view of the above-mentioned criteria and the responsibility which cloud customers as data controllers have, a careful selection of a cloud provider should be of an outmost importance to prospective cloud customers. The choice of a reputable cloud service provider helps, inter alia, to ensure a high standard of protection of personal data stored in the cloud and to minimize the exposure to potential penalties imposed by data protection supervisory authorities. In order to demonstrate a particular level of security and proper data management, cloud customers increasingly require from their cloud providers various levels and forms of widely recognized industry certifications; the generic standards such as ISO 27001 and 27002 which describe the steps to be taken in maintaining physical and online security, and steps to be taken in responding to breaches, are just one of them.

OTHER DATA IN THE CLOUD

Apart from personal data, the regular user of cloud services stores in the cloud an abundance of non-personal data as well. As these are often business sensitive data, the relevance of protecting them should not be overlooked. It is not uncommon for cloud customers to require, and cloud providers to commit to, the same level of protection to be awarded to such non-personal proprietary data as is guaranteed with respect to personal data.

The devil is in the detail and cloud contracts often contain provisions which, albeit relatively innocent at first glance, may give the cloud provider broad rights beyond what is strictly required for pure data processing operations, potentially allowing an uncontrolled use (and possibly monetization) of the controller's data by the processor. Even in standard cloud services agreements one may come across very aggressive provisions allowing for data mining, often disguised in a customer-friendly language that promises, for example "provision of targeted and customized content."

Recent developments surrounding the "Snowden" affair have highlighted the controversial question of access of state authorities to data stored in the cloud. The industry has reacted to those revelations and some cloud providers advocate reforms in government surveillance practices, clearer rules and greater transparency; some publish information – to the extent allowed – about volume, type, and impact of demands for customer data[2]; they share source codes to help customers reassure themselves that there are no 'back doors' through which state authorities would access their data, and strengthen encryption, among other measures. In order to guarantee a maximum

security that cloud customer's data will not be handled arbitrarily and without his knowledge, it is appropriate to agree with the cloud provider on detailed rules covering such requests and embed an obligation of the cloud provider to ascertain that the relevant state authority is indeed entitled to perform the given power.

CLOUD IN SPECIFIC SECTORS

When it comes to sector-specific regulation, it may be generally concluded there is no sector in which the use of cloud services would *a priori* be in conflict with the law. In some sectors such as banking, health care or public sector, specific obligations and rules may apply, which must be taken into account when purchasing cloud services. Sector-specific regulation typically revolves around issues such as risk assessment, specific requirements for a cloud contract (in particular around security), contingency planning and exit policy, and explicit ability of the sectoral cloud customer or its regulator to effectively inspect and audit the outsourced data processing activities, systems and facilities.

It has become common for large, multinational cloud providers to certify their data processing operations and facilities; in this regard, the new ISO 27018 certification will likely set the new industry standard. Where a cloud customer is contracting with a smaller cloud provider, he may have to invest more time and resources into examining thoroughly the level of security in order to satisfy himself that adequate security requirements are met.

Cloud products offered by reputable cloud services providers that are available in the market tend to abide by "privacy by design principle", i.e. are designed in such a way as to be in accord with legislation on personal data protection. Individual contractual models may differ significantly depending on where the personal data are transferred and the scope of empowerment of cloud providers in relation to users' data stored in the cloud. A thorough review of specific contract conditions as well as of specific sector requirements, where applicable, is a 'must' for a diligent cloud customer. Last but not least, cloud customers should also bear in mind that IT security in the context of cloud services significantly differs from the classical model of ICT services and these differences should be reflected in the contractual terms between cloud providers and cloud customers.

2 See, for example, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ or http://www.google.com/transparencyreport/removals/government/

GENERAL REQUIREMENTS
BASED ON EU DATA PRIVACY LAW

COUNSEL DETAILS:

Attorney: Lenka Suchánková
Law Firm: PIERSTONE s.r.o., advokátní kancelář
Na Příkopě 9
110 00 Prague 1
Czech Republic
Website: www.pierstone.com
E-mail: lenka.suchankova@pierstone.com

The below table aims to identify the most relevant data protection issues a customer should be aware of and assess before choosing a cloud provider. It does not attempt to provide a comprehensive overview of European data protection requirements or any other applicable laws.

The following responses are provided on the basis of the EU Data Protection Directive as well as the Cloud Opinion, and other sources explicitly cited. Where the Draft EU Data Protection Regulation foresees a considerable change it is explicitly mentioned.

INTRODUCTION

1

What is the definition of "personal data"? Is encrypted data regarded as personal data in case the cloud provider does not possess access to the encryption key?

Personal data are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[1]

There is currently no conclusive decision or guidance on the EU level on when encrypted data may be safely regarded as anonymized data and thus outside of scope of personal data protection[2]. The Draft EU

Data Protection Regulation is anticipated to explicitly regulate the use of anonymized data. The current Draft EU Data Protection Regulation states that principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. It may thus be conclude that when cloud providers have no access to the decryption key and no means 'reasonably likely' to be used for decryption, the encrypted data that they handle should not be considered personal data; rather, such data should be considered anonymous.

2

What are the key criteria to establish the applicability of EU data protection laws?

EU data protection laws apply to all data controllers (cloud customers) with one or more establishments within the EU as well as to all data controllers who are outside the EU but use equipment located within the EU to process personal data, unless such equipment is used only for purposes of transit through the territory of the EU.

CUSTOMER / CLOUD PROVIDER / SUB-PROCESSOR - ROLES AND RESPONSIBILITIES

3

In general, who is the data controller and who is the data processor in a cloud computing service? Describe their key obligations.

Typically, a cloud customer is the data controller: he determines the ultimate purpose of the processing and decides on the delegation of all or part of the processing activities to an external organization (cloud provider).

A cloud provider is generally considered a data processor who processes

1 See definition of personal data in Article 2 (a) of EU Directive 95/46/EC.
2 For example, the Cloud Opinion states that while encryption may significantly contribute to the confidentiality of personal data if implemented correctly, it does not render personal data irreversibly anonymous. On the other hand, WP 29 *Opinion 4/2007 on the concept of personal data states that one-way cryptography generally renders data anonymous, i.e. non-personal: "Disguising identities can also be done in a way that no reidentification is possible, e.g. by one-way cryptography, which creates in general anonymized data".* Further comments about the effectiveness of the procedures seem to suggest that the key factor determining whether encrypted data can be considered anonymous data is the reversibility of the one-way process.

personal data on behalf of the customer (data controller). There may, however, be situations in which a cloud provider may be considered either a joint controller or a controller in its own right, e.g. when the cloud provider processes personal data for its own purposes.

The cloud customer remains fully responsible for the legality of the data processing. Cloud providers are obliged to maintain confidentiality of personal data and may only process personal data on instructions from the controller (customer), unless they are required by law to process it for any other purpose. Cloud providers as data processors are further responsible for adopting technical and organizational security measures (see question 5), and must support and assist the data controller in complying with data subjects' rights.

4

Is a data processing agreement necessary between a customer and cloud provider? Describe its minimum content.

Yes. The agreement should stipulate in particular that (i) the processor may only act on instructions from the controller, and (ii) the obligations imposed on data controllers by the EU legislation shall also be incumbent on the data processor. These obligations include implementation of appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (see question 5).

5

Summarize the key technical and organizational measures that a cloud provider needs to comply with.

A cloud provider shall, in particular:

(i) Adopt reasonable measures to cope with the risk of disruptions, such as backup internet network links, redundant storage and effective data backup mechanisms;

(ii) Ensure integrity of personal data by employing intrusion detection / prevention systems;

(iii) Encrypt personal data in all cases when "in transit" and, when

available, data "at rest"[3], encryption should also be used for communications between cloud provider and the customer as well as between data centers;

(iv) Govern adequately rights and roles for accessing personal data and review them on a regular basis;

(v) Guarantee portability of data;

(vi) Implement other measures such as identification of all data processing operations, responding to access requests, allocation of resources, including designation of data protection offices responsible for data protection compliance, and maintain documentary evidence of such measures.

A cloud provider may demonstrate its compliance with data protection standards and implementation of appropriate and effective security measures by an independent third party audit or certification, provided that such audit is fully transparent.

6

Is the use of sub-processors by the cloud provider permissible?

Yes, cloud providers are generally allowed to subcontract services out to sub-processors, prior consent of the data controller is however required. Such consent may be given at the beginning of the service with a clear duty for the data processor to inform the data controller of any intended changes concerning the addition or replacement of sub-processors. The data controller should at all times retain the possibility to object to such changes or to terminate the contract.

3 The Cloud Opinion also states that in some cases (e.g., an IaaS storage service), a cloud client may not rely on an encryption solution offered by the cloud provider, but may choose to encrypt personal data prior to sending them to the cloud. The wording of the Cloud Opinion ("where available") suggests that the Cloud Opinion recognizes that encryption may not always be a feasible solution.

INTERNATIONAL DATA TRANSFERS

7

What are the requirements to transfer personal data within the EEA?

There are no specific requirements for transfer of personal data within the EEA.

8

What are the requirements to transfer personal data outside the EEA?

Personal data can only be transferred to third countries if such third countries ensure an adequate level of protection. If such adequacy of the protection of personal data in a third country in question is not recognized by a decision of the Commission regarding that particular country, the data controller can rely on the following transfer mechanisms:

(i) EU-US Safe Harbor Framework: Transfers of personal data to US organizations adhering to the principles of Safe Harbor can take place lawfully under EU law since the recipient organizations are deemed to provide an adequate level of protection to the transferred personal data. According to the Cloud Opinion, however, sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of the principles in the cloud environment. This is why some cloud providers offer additional safeguards such as the EU Standard Contractual Clauses.

(ii) EU Standard Contractual Clauses: Parties of the transfer (the EU-based data controller and exporter of data and the third country-based data processor and importer of the data) may conclude the EU Standard Contractual Clauses, which are deemed to offer adequate safeguards with respect to personal data protection, corresponding to the EU Data Protection Directive.

(iii) Binding Corporate Rules ("BCR"): BCR constitute a code of conduct for companies which transfer data within their group and may be used also in the context of cloud computing when the cloud provider is a data processor. In practice, BCR are rarely used by cloud customers and cloud providers as their applicability is limited to intra-group data processing.

SPECIAL CATEGORIES OF DATA ("SENSITIVE DATA")

9

What does the EU Data Protection Directive define as "sensitive data"? How can sensitive data be processed?

The EU Data Protection Directive provides for a specific data treatment of so-called "special categories of data" which it defines as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." Such specific categories of data (commonly referred to as "sensitive data") may only be processed either (i) with the explicit consent of the data subject, or, (ii) without such explicit consent, only if one of the specific conditions stipulated in the EU Data Protection Directive is met. The latter include, for example, processing that is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law; processing that is necessary to protect the vital interests of the data subject; processing that relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims; or processing of health data by health professionals in the context of medical treatment or health-care services.

For data transfer purposes, sensitive data are generally treated as any other personal data (for cross-border transfer requirements, see response to question 7 and 8). This is true also with respect to, specifically, health and medical data. This conclusion is supported by the Council of Europe Recommendation No. R (97) 5 on the Protection of Medical Data which provides in its Article 11 that *"the transborder flow of medical data to a state which has ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and which disposes of legislation which provides at least equivalent protection of medical data, should not be subjected to special conditions concerning the protection of privacy."* The Recommendation further states that *"where the protection of medical data can be considered to be in line with the principle of equivalent protection laid down in the convention, no restriction should be placed on the transborder flow of medical data to a state which has not ratified the convention but which has legal provisions which ensure protection in accordance with the principles of that convention and this recommendation."*

If sensitive data are to be transferred under the EU Standard Contractual Clause to third countries not providing adequate protection, the data exporter must ensure that the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection.

OTHER REQUIREMENTS

10

Is it permissible for a cloud provider to mine customer data for advertising purposes?

No. Personal data must always be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The data controller (cloud customer) must determine the purpose(s) of the processing when collecting personal data from the data subject and inform the data subject thereof. The cloud provider may only process the data for these approved purposes upon the instruction of the cloud customer.

11

Summarize the key aspects that cloud providers should be transparent about to their customers according to the Cloud Opinion.

Key aspects of transparency include:

(i) Relationship between the customer, cloud provider and sub-contractors (if any); the customer must be informed of all sub-processors and all locations where the processing may take place (notably if located outside of EEA), the type of service subcontracted, the characteristics of current or potential sub-contractors and of the guarantees that these entities offer to the provider of cloud computing services to comply with the EU Data Protection Directive.

(ii) Technical and organizational measures implemented by the provider; the cloud customer should specifically be informed about installation of any software on the customer's systems (e.g. browser plug-ins) by the cloud provider and its implications from the data protection and data security point of view.

12

Is an audit by an independent third party chosen by the cloud provider sufficient in lieu of an individual right to audit for the cloud customer?

Yes. The Cloud Opinion recognizes that individual audits of data hosted in a multi-party, virtualized server environment may be impractical technically and can in some instances serve to increase risks to those physical and logical network security controls in place. It concludes that in such cases, a relevant third party audit chosen by the controller may be deemed to satisfy the audit requirement and may be used in lieu of an individual controller's right to audit. Independence and transparency of such audit must be ensured.

PUBLIC SECTOR

13

Are there any different data protection requirements applicable to cloud customers from the private or public sector?

No. The EU Data Protection Directive does not distinguish between public and private sector data controllers (cloud customers).

(i) The Cloud Opinion states, in its recommendations on future developments, that special precautions may be needed for the deployment of cloud solutions by the public sector: Public bodies should first assess whether the communication, processing and storage of data outside national territory may expose the security and privacy of citizens and national security and economy to unacceptable risks – in particular if sensitive databases (e.g. census data) and services (e.g. health care) are involved. This special consideration should be given, at any rate, whenever sensitive data are processed in the cloud context. The Cloud Opinion concludes that *"from this standpoint, consideration might be given by national governments and EU institutions to further investigate the concept of a European Governmental cloud as a supra national virtual space where a consistent and harmonized set of rules could be applied."* The specifics of Governmental clouds are also dealt with in the ENISA paper on Security & Resilience in Governmental Clouds (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport)

and ENISA report from November 15, 2013 on Good Practice Guide for securely deploying Governmental Clouds (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds/).

GUIDANCE NOTES AND RECOMMENDATIONS

14

What guidance by EU data protection authorities is available on cloud computing?

Please see:

(i) Opinion 05/2012 on cloud computing released by the WP 29 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf);

(ii) Opinion 1/2010 on the concepts of "controller" and "processor" released by the WP 29 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

Further guidance may be sought in the following materials:

(iii) Working Paper on Cloud Computing - Privacy and data protection issues ("Sopot Memorandum") issued by the International Working Group on Data Protection in Telecommunications, of 24 April 2012 (http://germanitlaw.com/wp-content/uploads/2012/04/Sopot-Memorandum1.pdf)

(iv) Cloud Computing Risk Assessment analysis issued by European Union Agency for Network and Information Security (ENISA), of 20 November 2009 (http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment)

15

What are the key recommendations of the WP 29 for cloud customers in its Cloud Opinion?

The key recommendations of the WP 29 to cloud customers are the following:

(i) A comprehensive and thorough **risk analysis** should be performed prior to use of cloud computing; special attention should be paid to assessment of legal risks regarding data protection, concerning mainly security obligations and international transfers;

(ii) **Transparency** must be ensured. The cloud customer should be informed of all **sub-contractors** contributing to the provision of the respective cloud services and **all locations where personal data may be stored** or processed (notably if outside of EEA). Such sub-processing may only take place upon prior consent of the customer. The customer should obtain meaningful information about technical and organizational measures implemented by the cloud provider;

(iii) The customer must ensure that compliance with **purpose specification and limitation principles** i.e. ensure that personal data be processed only for the purposes determined by the customer as a data controller.

COUNTRY SPECIFIC REQUIREMENTS
BASED ON LOCAL PRIVACY LAW

POLAND

COUNSEL DETAILS:

Country: Poland
Attorney: Agata Szeliga
Law Firm: Sołtysiński Kawecki & Szlęzak
ul. Wawelska 15 B
02-034 Warszawa
Poland
Website: www.skslegal.pl
E-mail: office@skslegal.pl

The following briefly outlines the non-sector-specific data protection requirements that organizations or institutions need to bear in mind in relation to their use of cloud computing. Please read the following table together with the table which spells out the general requirements under EU data privacy law (see *supra*).

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data?

Act of 29 August 1997 on the Protection of Personal Data (the "Privacy Act"). The English version of the Privacy Act is available at http://www.giodo.gov.pl/plik/id_p/193/j/en/.

The Privacy Act is substantially identical with the EU Data Protection Directive. Where sector-specific legislation provides for a higher level of personal data protection, it will prevail over the Privacy Act. Such sector-specific legislation that may be relevant for cloud computing is the Telecommunications Act, the Labor Code, the Banking Law, Insurance Act, as well as the set of laws concerning medical documentation (e.g. the Act on Patients Rights).

2

Which authority oversees the data protection law? Summarize its powers.

Full name: Główny Inspektor Ochrony Danych Osobowych (General Inspector of Personal Data Protection)

Address: ul. Stawki 2 00-193 Warszawa, www.giodo.gov.pl

The DPA's powers include:

(i) Supervision and inspections to ensure and assess the compliance of data processing with the Privacy Act, including the right to access facilities, both private and public, where data systems or personal data is kept or processed;

(ii) issuing administrative decisions (in particular, approving the transfer of personal data to third countries or issuing post-inspection decisions) and reviewing complaints with respect to the enforcement of the Privacy Act;

(iii) issuing administrative decisions by which the DPA orders the addressee to restore the proper legal status, in particular, through: completion, updating, correction, disclosure (or non-disclosure), deletion of personal data; or suspension of data transfer to third countries.

(iv) cooperation with law enforcement authorities if the DPA comes to the conclusion that a given act or omission constitutes a criminal offence;

(v) keeping a register of data systems and providing information about registered data files;

(vi) issuing opinions on bills and regulations concerning protection of personal data.

Generally, the DPA will only have authority over cloud customers and cloud providers located in Poland. The DPA will have authority over data processing that occurs on the territory of Poland even if the data

controller – cloud customer is established outside the territory of the EU/EEA but carries out processing on the territory of Poland using technical equipment located in Poland, unless where it is merely a transit through the territory of the European Union.

It is sometimes disputed whether the Privacy Act properly implements Art. 4 (1)(a) of the EU Data Protection Directive in regards to the Privacy Act application to Polish "establishments" of data controllers from the EEA. Most legal commentators agree that the interpretation in compliance with EU Data Protection Directive requires that the Privacy Act is applied to the Polish branches or representative offices of data controllers from the EEA, while the head offices operations are subject to the law applicable to their seat. Thus, such core operations outside of Poland are not subject to the DPA authority.

3

Identify the requirements for the applicability of local data protection laws.

The criteria generally correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section, however, as noted in response to question 2 above, there are some discussions around the application of the definition of "establishment" of data controllers.

CLOUD CUSTOMER / CLOUD PROVIDER / SUB-PROCESSOR - ROLES AND RESPONSIBILITIES

4

Are there any local law requirements with respect to data processing and a data processing agreement that go beyond the requirements of the EU Data Protection Directive?

Yes. The data controller is obliged to appoint a data protection officer in its organization. This obligation applies to all organizations, provided that in case of individual entrepreneurs, such individual may act as the data protection officer.

The Privacy Act elaborates on the general requirements of the EU Data Protection Directive for a written data processing agreement to be

signed between a data controller and a data processor for purposes of each data processing relationship, by prescribing the following minimum content requirements: specification of categories of data processed, the purpose of the processing, and contractual safeguards of the data processor regarding technical and organizational security of the personal data which shall include, in particular, security policy and the IT system management instruction (see response to question 5).

5

List the technical and organizational measures set forth by the Privacy Act, if any.

Detailed security requirements are specified in the Ordinance of Minister of Internal Affairs and Administration on data processing documentation, as well as technical and organizational measures which should be met by equipment and IT systems used for processing of personal data. Data controllers and data processors are required to:

(i) implement a security policy that should contain, in particular, a list of buildings or premises where personal data is processed, the list of data systems and the software used for processing, a description of the structure of data systems, flow of data between various systems, or measures which are implemented in order to ensure confidentiality, integrity and accountability of processed data.

(ii) implement an IT system management instruction that specifies, in particular, the procedures for granting authorization for data processing and recording that information in IT systems, as well as the person responsible for these tasks, authorization methods, backup copy procedures, and where and for how long the media with personal data and backup copies are stored. Detailed guidelines concerning the content of these documents have been adopted by the DPA and are available on its website.

(iii) establish applicable security measures (out of three security levels):

(a) basic – when only non-sensitive data is processed and none of the IT system devices are connected to a public telecommunications network;

(b) increased – if sensitive data is processed and none of the IT system devices are connected to a public telecommunications network;

(c) high – if at least one device of an IT system used to process data is connected to a public telecommunications network.

INTERNATIONAL DATA TRANSFERS

6

Does local law or regulation require notification to or approval from the DPA for data transfers outside the EEA based on EU Standard Contractual Clauses or Safe Harbor?

Yes. The approval of the DPA for the transfer of personal data to a third country which does not ensure an adequate level of personal data protection is required even if the data importer and data exporter have entered into the EU Standard Contractual Clauses. However, execution of the EU Standard Contractual Clauses usually simplifies the proceedings before DPA as it is perceived as a measure which ensures adequate safeguards for personal data.

DPA approval is not currently required for transfers of personal data to U.S. entities participating in the EU-US Safe Harbor Framework. It can be reasonably expected that, in light of the recent EU Commission's reservation to the EU-US Safe Harbor Framework, the DPA will follow suite and reconsider its stance to the EU-US Safe Harbor Framework.

The data controller must file application to the DPA requesting the approval of the transfer; the application, including all attachments must be in Polish. If the transfer is based on the EU Standard Contractual Clauses, the approval process may take up to approximately 3 to 5 months (but may also be considerable shorter if the DPA is familiar with the standard agreements of a certain cloud provider). There is legislation pending that will no longer require approval for a data transfer based on EU Standard Contractual Clauses (see response to question 14). The application is subject to an administrative fee in the amount of 17 PLN (approx. 3,5 EUR).

7

Describe any requirements with respect to transfer of personal data outside the EEA that go beyond the requirements set out by the EU Data Protection Directive.

There are no further requirements in this regard.

SPECIAL CATEGORIES OF DATA ("SENSITIVE DATA")

8

Are there any local law requirements with respect to sensitive data that go beyond the requirements of the EU Data Protection Directive?

Yes. The Privacy Act defines sensitive data quite broadly as to include, explicitly, also data related to the administrative and civil law proceedings, data about addictions, or data about genetic code.

In practice, the DPA applies quite stringent rules to the transfers of sensitive data to third countries which do not ensure adequate level of protection. The application for approval of such transfer is reviewed in more detail and consequently, the approval process is longer than in case of non-sensitive data.

If sensitive data are processed in IT system, the system must comply with requirement for at least "increased" level of security (see response to question 5 above).

FINANCIAL DATA

9

Briefly summarize the key sector-specific legal and regulatory requirements that apply to financial data that financial institutions need to be aware of, if they wish to use cloud computing, if any.

The applicable sector-specific regulation includes:

(i) Banking Law of 29 August 1997 (the "Banking Law ") – applicable to all banking entities operating in Poland;

(ii) Act of 29 July 2005 on Trading in Financial Instruments (the "ATFI")

– applicable to all investment firms operating in Poland, including brokerage bureaus of Polish banks and, following interpretation of the local regulator, to banks pursuing certain investment activities based on their banking license.

(iii) Act of 22 May 2003 on Insurance Activity (the "Insurance Act") applicable to insurance companies and insurance intermediaries.

Neither of these acts regulates cloud computing directly; they are nevertheless applicable to outsourcing. However, it is generally accepted by both the financial institutions and the regulator, the Polish Financial Supervision Commission, that the rules on outsourcing would apply to the deployment of cloud computing by the financial institutions. There is however a possibility that depending on the concrete business scenario (e.g. category of data entrusted to the cloud provider, no access to the content of data by the cloud provider due to the encryption) certain agreements for cloud services may not be classified as outsourcing.

The outsourcing rules specific to banking and brokerage activities apply when customer data are processed (i.e., they do not apply to outsourcing of purely internal systems such as payroll or HR) and/or the service is necessary for efficient bank's and/or investment firm's operation (email systems might be regarded as such systems). Moreover, some restrictive requirements applicable to banks using cloud computing result from recommendations issued by the Polish Financial Supervision Commission.

The key requirements are the following:

(i) outsourcing may not result in limitation of the service provider's liability towards the financial institution for damage caused to its clients due to non-performance or improper performance of the outsourcing agreement by the service provider or its subcontractors;

(ii) chain outsourcing (i.e. number of outsourcing subcontractors) is either limited (for banks) or prohibited (for investment firms);

10

Are there any notifications to or approvals on the use of cloud computing from the applicable regulator required?

Yes. Pursuant to the Banking Law and ATFI, a bank / an investment firm needs to obtain the Polish Financial Supervision Commission's approval to conclude outsourcing agreement with a service provider based outside of the EEA, or if such agreement provides that the services will be performed outside of the EEA. The approval procedure may take up to approximately 6 to 12 months (but may also be considerable shorter if the Financial Supervision Commission is familiar with the standard agreements of a certain cloud provider). This approval is in addition to any approval that may be required from the DPA for personal data transfer (processing) in third countries which do not ensure an adequate level of personal data protection (see response to question 6 above).

The Insurance Law does not establish any approval / notification procedure.

OTHER REQUIREMENTS

11

Explain if under the Privacy Act it would be permissible for a cloud provider to mine customer data for advertising purposes.

No, it would not be permissible. Assuming that the cloud provider will be in the role of a data processor, the principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

This principle is usually reflected in the wording of data processing agreements which often state explicitly that the processor is not allowed to use the entrusted personal data for other purposes than those specified in the agreement.

12

Is the cloud provider under the Privacy Act required to be transparent as outlined in question 11 of the EU Data Privacy Law section?

Yes. The DPA applies the rules of the Cloud Opinion.

GUIDANCE NOTES AND RECOMMENDATIONS

13

Is there any local guidance on cloud computing issued by the Commission in addition to the Cloud Opinion?

Yes. The DPA issued a document titled "Ten Commandments" for the application of cloud-based services by public administrations. This is an unofficial and non-binding document, however, it could be expected that the public institutions would follow the DPA guidance.

The text is available at http://giodo.gov.pl/259/id_art/6271/j/pl

PENDING LEGISLATION

14

Is there any pending legislation that will have a major impact on cloud computing?

Yes. A draft of the Act on Facilitation of a Business Activity, which will amend the Privacy Act and which is currently at the stage of inter-ministerial consultations, provides that:

(i) the data controller will have the right, instead of the present obligation, to appoint a data protection officer. The duties of the officer will be determined in more detail. The data controller will be obligated to notify the DPA of the appointment and dismissal of the officer. The DPA will maintain the national register of notified officers.

(ii) The data controller who appointed the data protection officer and notified the DPA of his/her appointment will not be subject to the obligation to register the data system in which non-sensitive data is processed.

(iii) the new law will waive the present obligation to apply for the DPA's approval for the transfer of personal data outside of the EEA to a third country which does not ensure an adequate level of personal data protection if the controller adopts EU Standard Contractual Clauses, or if the controller implements binding corporate rules ('BCRs') approved by the DPA. The rules applicable to the approval of the BCRs are specified in the new law.

There is also pending a major sector-specific bill on processing of healthcare data which will amend the Act on Information Systems in Healthcare and the Act on Patients' Rights. The Government also plans to modify the rules applicable to electronic medical documentation. One of the objectives of the proposed legislation is to that any processing of medical documentation may be entrusted to third parties based on the same rules applicable to entrusting the processing of personal data specified in the Privacy Act, i.e. data processing agreement which determines the scope and purpose of processing; appropriate technical and organizational measures, etc.