CLOUD COMPUTING IN EASTERN EUROPE

SURVEY OF REGULATORY FRAMEWORKS

TABLE OF **CONTENT**

FOREWORD

We are pleased to introduce to you this Cloud Computing in Eastern Europe – Survey of Regulatory Frameworks.

This publication addresses the most important legal issues relevant for legal practitioners and business people dealing with cloud computing products and services in 14 jurisdictions across the region.

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 in collaboration with the following reputable legal experts:

- **Bulgaria**, Nikolay Zisov, Boyanov & Co., Attorneys at Law
- **Croatia**, Olena Manuilenko, Vukmir & Associates, Attorneys-at-Law
- **Cyprus**, Anastasia Papadopoulou, Tassos Papadopoulos & Associates LLC
- **Estonia**, Hannes Vallikivi, Tark Grunte Sutkiene
- **Greece**, Takis Kakouris, Zepos & Yannopoulos
- **Hungary**, Dóra Petrányi, Márton Domokos, CMS Cameron McKenna LLP
- **Latvia**, Vineta Čukste, Kronbergs & Čukste Attorneys at Law
- **Lithuania**, Iraida Žogaitė, Paulius Zapolskis, Baltic Legal Solutions Lithuania
- **Malta**, Dr. Antoine Camilleri, Dr. Claude Micallef-Grimaud, Mamo TCV Advocates
- **Poland**, Agata Szeliga, Sołtysiński Kawecki & Szlęzak
- **Romania**, Andreea Lisievici, Țuca Zbârcea & Asociații
- **Slovenia**, Nastja Rovšek Srše, Law Firm Kanalec Ltd.

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 country-specific questionnaires describing key data protection requirements relevant to cloud computing under the laws of the selected EU Member States.

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:

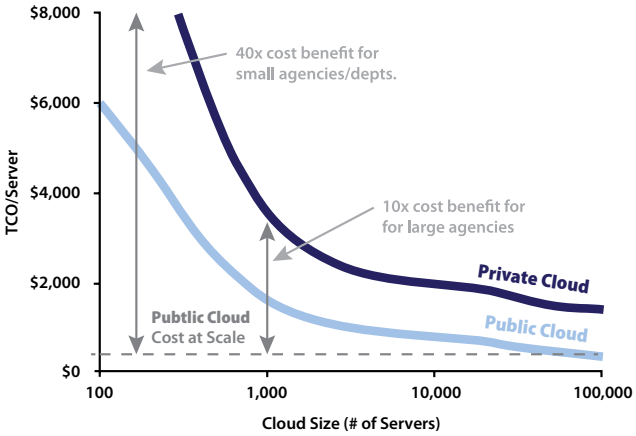


Figure 1: Cost per managed server – Small enterprise, Private, Public clouds[2]

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

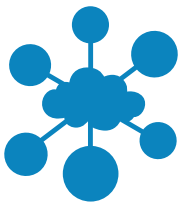
According to IDC research from Dec. 2013[4], the fastest growing segment of cloud services globally will be SaaS - it is predicted to grow nearly five times faster than the software market as a whole. By 2016, nearly $1 of every $6 spent on packaged software, and $1 of every $5 spent on applications, 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

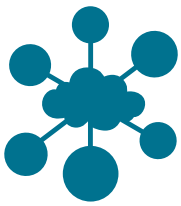
What are the key recommendations of the WP 29 for cloud customers in its Cloud Opinion?

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

BULGARIA

COUNSEL DETAILS:

Country: Republic of Bulgaria
Attorney: Nikolay Zisov
Law Firm: Boyanov & Co., Attorneys at Law
82, Patriarch Evtimii Blvd.
Sofia 1463
Republic of Bulgaria
Website: www.boyanov.com
E-mail: mail@boyanov.com

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?

The Personal Data Protection Act (Закон за защита на личните данни), promulgated in State Gazette issue 1 of January 4, 2002, as amended (hereinafter referred to as the "Privacy Act"). The Privacy Act is substantially similar to the EU Data Protection Directive and implements it in the national law. The Privacy Act is available in English language (unofficial translation) on the website of the DPA at: https://www.cpdp.bg/en/index.php?p=element&aid=373.

Other relevant pieces of legislation are the Regulation on Activity of the Personal Data Protection Commission and its Administration, as well as Ordinance No. 1 dated 30.01.2013 on the Minimum Level of Technical and Organizational Measures and the Admissible Type of Personal Data Protection.

2

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

Комисия за защита на личните данни ("Personal Data Protection Commission", hereinafter referred to as "DPA").

Address: 2, Prof. Tzvetan Lazarov Blvd., Sofia 1592;

www.cpdp.bg; email: kzld@cpdp.bg.

The DPA is an independent governmental body responsible for the protection of the individuals in the processing of their personal data and the access to such data and for ensuring compliance with the Privacy Act.

The DPA oversees compliance with the statutory provisions in the field of personal data protection. It is entitled to perform investigations (including on-site investigations), to issue decisions on administrative offences under the Privacy Act, and to impose fines and other measures for its violations. The DPA reviews and decides on complaints regarding alleged violations of the Privacy Act. It may also issue mandatory instructions to data controllers. Furthermore, the DPA keeps register of data controllers and of the registers kept by them.

The DPA will have authority over cloud customers and cloud providers located in the territory of Bulgaria. The DPA will have authority over data processing that occurs on the territory of Bulgaria even if the data controller – cloud customer is established outside the territory of the EU (e.g. in the USA) but carries out processing on the territory of Bulgaria through a local data processor – cloud provider (unless where it is merely a transit through the territory of the European Union).

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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?

The Privacy Act provides for a joint and several liability of the data processor (cloud provider) and data controller (cloud customer) for damages caused to third parties through acts or omission to act by the data processor.

There are no other specific requirements going beyond the EU Data Protection Directive, certain requirements are however stipulated in more detail.

5

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

The Privacy Act sets forth a general requirement that data controllers implement appropriate technical and organizational measures to protect the data. It also stipulates that where the processing involves the transmission of data over an electronic network (including in the case of use of cloud services), the data controller must implement special protection measures; these measures must take into account the current level of used technology and ensure a level of security corresponding to the risks involved in processing, and the nature of the data to be protected. The Privacy Act also requires that data controllers set fixed periods of time for conducting regular reviews of the need for processing and removal of personal data.

The minimum level of technical and organizational measures, as well as the admissible type of protection is specified in an Ordinance issued by the DPA (hereinafter the "Ordinance"). The measures pertinent to the protection of automated IT systems and networks, include, inter alia, policy documents and data protection guidelines; identification and authentication mechanisms; registries management; virus protection, contingency planning; configuration management; creation of back-up copies for restoration; personnel training; or data removal/wipe-out procedures. With respect to encryption protection, the key measures

listed in the Ordinance include standard cryptographic capabilities of the operational systems, of the database management system and the communication equipment; further encryption measures include systems for allocation and management of encryption keys and electronic signatures.

In order to properly determine which measures should be implemented, data controllers should first assess the level of impact of potential breach of privacy ("extremely high", "high", "medium" and "low").

INTERNATIONAL DATA TRANSFER

6

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

Yes. The DPA's approval is required for data transfers outside the EEA based on EU Standard Contractual Clauses or Safe Harbor. In this case, however, the DPA does not make an assessment of the adequacy of the level of protection of personal data afforded by the third country.

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 such additional requirements.

8

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

No. The rules and requirements largely mirror the provisions of the EU Data Protection Directive.

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.

Recently adopted changes to the Credit Institutions Act (promulgated in State Gazette on March 23, 2014) implement the outsourcing rules applicable to banks introduced by the Capital Requirements Directive (Directive 2013/36/EU). These amendments grant the local bank supervisory authority (the Bulgarian National Bank) investigatory powers described in Article 65 (3) of the Capital Requirements Directive, including the right to require information and documents, access IT systems, examine the records and obtain explanations and conduct inspections at the business premises of financial institutions and any third parties to whom the institutions have outsourced operational functions or activities (including cloud services providers).

Payment service providers must also comply with the Payment Services and Payment Systems Act which requires them, inter alia, to process personal data of the users of payment services in compliance with the Privacy Act. For the purposes of prevention, investigation and detection of fraud related to payment services, the processing may be done without the consent of the data subject.

10

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

No special notification or approval on the use of cloud computing provider by financial institutions is required.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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?

While the Privacy Act does not explicitly elaborate on the transparency requirement, cloud customers and providers who wish to be fully compliant should apply the principles as outlined in response to question 11 of the EU Data Privacy Law sections.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No such guidance has been issued to date.

PENDING LEGISLATION

14

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

There is no currently pending legislation that is expected to have major impact on cloud computing.

CROATIA

COUNSEL DETAILS:

Country: Croatia
Attorney: Olena Manuilenko
Law Firm: Vukmir & Associates, Attorney-at-Law
Gramača 2L
10000 Zagreb
Croatia
Website: www.vukmir.net
E-mail: kmir@vukmir.net

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?

Personal Data Protection Act (Official Gazette No. 106/12 – Consolidated text; hereinafter: the Privacy Act)[1]. The Privacy Act is fully harmonized with the EU Directive, thus it is substantially identical with the EU Directive. There are two Regulations adopted pursuant to the Privacy Act, which elaborate upon the required formalities and protective measures relating to data processing: Regulation on the Manner of Keeping the Records of Personal Data Filing Systems and the Pertinent Records Form (the Official Gazette No. 105/04)[2]; and the Regulation

1 An unofficial English translation is available at the official website of the national Data Protection Agency as a downloadable Word document: http://www.azop.hr/page.aspx?PageID=79 (last link at the bottom of the webpage)
2 English translation is available at the official website of the national Data Protection Agency: http://www.azop.hr/page.aspx?PageID=79

on the Procedure for Storage and Special Measures Relating to the Technical Protection of Special Categories of Personal Data (the Official Gazette No. 105/04)[3].

2

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

Agencija za zaštitu osobnih podataka (AZOP; eng. Personal Data Protection Agency; hereinafter: the DPA)

Martićeva 14, 10000 Zagreb, CROATIA

Tel.: +385 1 4609 000; Fax. +385 1 4609 099; E-mail: azop@azop.hr;

Web: http://www.azop.hr (partially available in English).

The DPA is an independent administrative authority responsible to the Croatian Parliament. The Privacy Act applies to all data controllers (cloud customers) established in Croatia, as well as to all data controllers who are established outside Croatia, but use equipment located within Croatia to process personal data, unless such equipment is used only for purposes of transit through the territory of the EU.

The DPA performs the following activities: (i) supervises the implementation of personal data protection (inspections upon request of the data subject, a third party or ex officio); (ii) draws attention to data processing violations discovered and publishes its significant decisions; (iii) compiles a list of countries and international organizations that provide for an adequate level of personal data protection; (iv) decides upon data processing violation reports; (v) maintains the Central Personal Database Register.

Further, the DPA (i) monitors the regulation of personal data protection and cooperates with competent data protection authorities in other countries; (ii) monitors the transfer of personal data outside Croatia;

3 English translation is available at the official website of the national Data Protection Agency: http://www.azop.hr/page.aspx?PageID=79

(iii) develops methodological recommendations for the advancement of personal data protection; (iv) monitors the application of organizational and technical measures aimed at data protection and proposes improvements of such measures.

Should any violations be determined, the DPA is entitled to warn data controllers, data processors or data recipients about the irregularities by issuing decisions whereby it is ordered that any irregularities must be eliminated within a certain time period. The DPA may propose competent authorities to initiate criminal or misdemeanor proceedings.

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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. In addition to the requirements of the EU Data Protection Directive, the Privacy Act prescribes, in particular that:

(i) the data processor must adopt a written internal resolution on the establishing any personal database in compliance with the Regulation on the Manner of Keeping the Records of Personal Data Filing Systems and the Pertinent Records Form;

(ii) the data processor must be registered for the provision of the data processing activities/services assigned to them by the data controller under the processing agreement;

(iii) the data processor must comply with the requirements determined

by special regulations governing the field of information security in case of classified data processing;

(iv) data controllers, data processors and data recipients must allow the DPA access to files and other documentation, as well as to electronic processing means, and must submit the requested files and other documentation based on a written request of the DPA.

(v) an international data processing contract must be preapproved by the DPA, if the data are transferred to an "unsafe" country, even if the contract is based on the EU Standard Contractual Clauses. On the other hand, Safe Harbor membership is deemed to provide sufficient level of protection. The contract must be submitted for approval in a Croatian translation;

(vi) if the data controller employs more than 20 employees must appoint a data protection officer in its organization and publicize report the name and contact details of the officer on its website, as well as register the officer with the DPA within one month from the appointment. The DPA maintains the Register of Personal Data Protection Officers.

5

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

There are no further requirements in this regard.

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?

Preapproval is only required for the use of Standard Contractual Clauses, but not for Safe Harbor. The data processing/transfer contract must be submitted to the DPA in a Croatian translation. No fee for the review and approval is charged by the DPA.

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. Detailed specific measures are prescribed for sensitive data in the Regulation on the Procedure for Storage and Special Measures Relating to the Technical Protection of Special Categories of Personal Data; *inter alia*:

(i) computers and other system components must be connected in accordance with the instructions of the respective equipment manufacturers and in line with valid technical standards;

(ii) the use of uninterruptible power supply devices is obligatory;

(iii) positioning, placing and installation of computers and computer

network must be performed by qualified personnel subject to the approval of the data controller and in compliance with the applicable standards and technical instructions;

(iv) the computer system processing sensitive data must have the following security mechanisms implemented: for secure logging in order to monitor and limit the computer access; for the prevention of unauthorized data export and import; for the protection from computer viruses and other malware; for encryption protection during the transfer of data;

(v) physical access to the rooms with computers and telecommunication equipment must be restricted; access to system data must be restricted to the authorized staff and authorized experts only; access to the telecommunication, computer and software system must be restricted by the use of appropriate unique user names and passwords;

(vi) any access to the data systems or records, as well as attempts of unauthorized system access, must be automatically recorded, indicating the user name, date and the log in and log out times;

(vii) proper measure for fire protection, protection from electrical and magnetic fields, from ionizing radiation, electrostatic electricity, humidity, cold and heat, corrosive and volatile liquids, explosives and similar substances, from dust, as well as safety measures in the event of earthquake or other natural disasters, war and imminent threat of war must be undertaken;

(viii) measures relating to the storage of system data on devices with removable storage must be performed on a daily, weekly, monthly and annual bases; a person authorized for the storage of data on devices with removable storage must be appointed; data stored on devices with removable storage must be kept in a safe place at least 20 km or 50 km from the building housing the personal data filing system, depending on the frequency of the storage;

(ix) devices with removable storage containing personal data filing

systems (backup copies) must be placed in a water- and fire-resistant safe.

(x) measures, procedures and staff authorized for system safety, storage and protection must be defined, implemented and controlled in accordance with the plan adopted by the data controller in line with the respective international recommendations (ISO 17799); etc.

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.

Subject to Article 388 of the Credit Institutions Act (Official Gazette No. 159/13) that entered into force on January 1, 2014, the Croatian National Bank's Resolution on Prudential Management of the Information System (Official Gazette No. 37/10) which dealt with information security standards in the financial sector has been substituted by the relevant provisions of the Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on Prudential Requirements for Credit Institutions and Investment Firms and Amending Regulation (EU) No 648/2012, effective from January 1, 2014, when the Regulation entered into force. Therefore, the EU-wide requirements set forth in the Regulation are directly applicable in Croatia.

There is no specific official guidance of the DPA on the subject matter topic.

10

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

There is no specific official guidance of the DPA/ Croatian National Bank on the topic of cloud computing and hence no notification obligation towards these authorities.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No, there is no specific official guidance of the DPA on the topic of cloud computing.

PENDING LEGISLATION

14

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

No.

CYPRUS

COUNSEL DETAILS:

Country: Cyprus
Attorney: Anastasia Papadopoulou
Law Firm: Tassos Papadopoulos & Associates LLC
2 Sofouli Street, Chanteclair Building,The Second Floor
Nicosia 1096
Cyprus
Website: www.tplaw.com.cy
E-mail: info@tplaw.com.cy

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 on the Processing of Personal Data (Protection of the Individual) of 23 November 2001, Law No. 138(I)/2001, as amended by the Processing of Personal Data (Protection of the Individual) (Amending) Law of 2 May 2003, Law No. 37(I)/2003 and the Processing of Personal Data (Protection of the Individual) (Amending) Law of 11 July 2012, Law No. 105(I)/2012 implemented the Data Protection Directive (the "Privacy Act"). The Privacy Act is substantially identical with the EU Data Protection Directive.

2

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

The Commissioner for the Protection of Personal Data.

Address: 1 Iasonos street, 2nd Floor, Nicosia 1082,

Email: commissioner@dataprotection.gov.cy

Website: www.dataprotection.gov.cy

The DPA is an independent central administrative body empowered to oversee compliance with the Privacy Act. The DPA is entitled to perform investigations (including on-site investigations), to issue decisions on administrative offences under the Data Protection Act, and to impose fines and other measures for its violations. DPA receives complaints regarding alleged violations of the Act and responds to them. Furthermore, the DPA maintains a register of personal data processing operations.

Generally, the DPA will only have authority over cloud customers and cloud providers located in the territory of the Republic of Cyprus. The DPA will have authority over data processing that occurs in the territory of the Republic of Cyprus even if the data controller – cloud customer is established outside the territory of the EU (e.g. in the USA) but carries out processing on the territory of the Republic of Cyprus through a local data processor – cloud provider (unless where it is merely a transit through the territory of the European Union).

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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. In furtherance of the purpose specification and limitation principle, the Privacy Act expressly prohibits combining personal data collected for different purposes.

There are no other specific requirements going beyond the EU Data Protection Directive.

5

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

The Privacy Act does not list any specific technical and organizational measures; it only sets forth the general obligation to implement appropriate technical and organizational measures to protect personal data having regard to the state of the art, the risks represented by the processing and the nature of the data to be protected. Processing must be confidential and may be carried out only by the data controller and others, upon the data controller's instructions and under its control, provided they possess the necessary technical skill and personal integrity.

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?

No.

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?

No. The rules and requirements largely mirror the provisions of the EU Data Protection Directive.

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.

According to the Directives Issued to Banks by the Central Bank of Cyprus on "The Framework of Principles of Operation and Criteria of Assessment of Banks' Organizational Structure, Internal Governance and Internal Control Systems" of 2006 to 2012 ("the Directives") , the provision of data storage services (physical and electronic) constitutes outsourcing. The Directives provide that any outsourcing by banks of the activities they are permitted to outsource (including any IT functions, which would most likely cover also cloud computing) must not result in decreased compliance with relevant legislation or limitation of control possibilities.

Appendix 1 of the Directives provides details about the requirements applicable to outsourcing and the agreement between the bank and the service provider. These include, for example, requirements on banks to:

(i) establish and maintain policies on outsourcing and ensure that outsourcing does not create an impediment in its ability to fulfill its obligations towards customers and the Central Bank of Cyprus, to oversee its outsourced activities, comply with legal and regulatory requirements, and impair the Central Bank's ability to supervise the business of the bank;

(ii) establish a comprehensive outsourcing risk management program to address the risks related to outsourced activities and its relationship with the independent outsourcing service provider.;

(iii) maintain contingency plans, including a disaster recovery plan, which should be tested periodically (the same applies to the service provider);

(iv) take steps to ensure that outsourcing service providers protect both the bank's and its customers' confidential information.

An outsourcing contract should:

(i) clearly define which activities are going to be outsourced, including appropriate service and performance levels;

(ii) not prevent or impede the bank from meeting its respective supervisory / regulatory obligations or the Central Bank of Cyprus from exercising its supervisory / regulatory powers;

(iii) allow the bank to retain the ability to access all books, records and information relevant to the outsourced activity;

(iv) provide for the continuous monitoring and assessment by the bank of the service provider so that any necessary corrective measures can be taken in a timely manner.;

(v) describe clearly and in detail all aspects of the exit policy, upon normal or abnormal contract termination.

(vi) address material issues unique to the outsourcing arrangement,

e.g. choice-of-law (where the provider is located abroad) and dispute resolution rules;

(vii) stipulate conditions of subcontracting of all or part of an outsourced activity. Where appropriate, the service provider should seek the approval of the bank, prior to assigning to subcontractors all or a part of the serviced activity.

10

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

Yes. Banks intending to proceed with the outsourcing of permitted activities (i.e. including IT activities) must notify in writing the Central Bank of Cyprus of the intended outsourcing.

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. Personal data cannot be processed for advertising or direct marketing purposes unless the data subject's consent has been obtained in writing.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No.

PENDING LEGISLATION

14

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

No.

CZECH REPUBLIC

COUNSEL DETAILS:

Country: Czech Republic
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 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 no. 101/2000 Coll., Act on personal data protection and on amendment of other laws, as amended (the "Privacy Act"). The Privacy Act is substantially identical with the EU Data Protection Directive.

An English version of the Privacy Act is available at http://www.uoou.cz/en/VismoOnline_ActionScripts/File.ashx?id_org=200156&id_dokumenty=1116

2

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

Úřad pro ochranu osobních údajů ("Personal Data Protection Office", hereinafter referred to only as the "DPA")

Address: Pplk. Sochora 27, 170 00 Praha 7; www.uoou.cz

The DPA is an independent central administrative body empowered to oversee compliance with the Privacy Act. The DPA is entitled to perform investigations (including on-site investigations), to issue decisions on administrative offences under the Privacy Act, and to impose fines and other measures for its violations. DPA receives complaints regarding alleged violations of the Act and responds to them. Furthermore, the DPA maintains register of personal data processing operations and provides consultations in the area of personal data protection.

Generally, the DPA will only have authority over cloud customers and cloud providers located in the territory of the Czech Republic. The DPA will have authority over data processing that occurs on the territory of the Czech Republic even if the data controller / cloud customer is established outside the territory of the EU (e.g. in the USA) but carries out processing on the territory of the Czech Republic through a local (Czech-based) data processor – cloud provider (unless where it is merely a transit through the territory of the European Union).

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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 Privacy Act explicitly provides for a joint and several liability of the data processor (cloud provider) and data controller (cloud customer) in certain circumstances. If a data processor discovers that the data controller is in breach of its statutory obligations, the data processor is obliged to notify the data controller thereof and terminate the processing immediately; otherwise, it becomes jointly and severally liable for damage caused to data subjects.

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: the scope and purpose of the processing, the term of the processing and contractual safeguards of the data processor (cloud provider) regarding technical and organizational security of the personal data.

In furtherance of the purpose specification and limitation principle, the Privacy Act expressly prohibits combining personal data collected for different purposes.

There are no other specific requirements going beyond the EU Data Protection Directive, certain requirements are however stipulated in more detail.

5

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

The Privacy Act is technologically neutral and as such does not list specific measures, however, it provide that the measures should include, *inter alia*, access control measures and measures that enable detection of the persons who received personal data; in case of automatic processing, access should be on the basis of specific user authorizations

established exclusively for the authorized persons, electronic records should be made enabling to identify and verify when, by whom and for what reason the personal data were recorded or otherwise processed, and any unauthorized access to the data carriers should be prevented. The implemented measures must be documented and must remain in place also after the processing has ended.

In addition, the notification form through which data controllers notify the DPA about intended personal data processing (available in an electronic form on the DPA's website) includes a list of measures from which the notifying controller may choose to tick those that it had implemented in its organization. This non-exhaustive list of measures includes the following: locks, bars, and other physical protection; electronic protection; security guidelines / documentation on adopted technical and organizational measures; central protection console; access rights; anti-virus protection; security backups; encryption.

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?

No. Apart from the general obligation to notify to the DPA any intended automated data processing operations, including any proposed transfers of data to third countries, prior to the very commencement of the data processing, no other specific ad hoc approval or notification to the DPA of a data transfer outside the EEA based on EU Standard Contractual Clauses or the EU-US Safe Harbor Framework is required. However, the DPA recommends on its website that data controllers who plan to transfer data under the EU-US Safe Harbor Framework consult the DPA to ascertain that the planned transfer is indeed covered by the European Commission's decision on EU-US Safe Harbor.

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?

No. The rules and requirements largely mirror the provisions of the EU Data Protection Directive.

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.

Decree 23/2014 of the Czech National Bank on the performance of the activity of banks, credit unions and investment firms ("CNB Decree 23/2014")[1] provides that any outsourcing by financial institutions of its activities (i.e. including any outsourcing of IT functions, which would cover also cloud computing; see next question) must not result in decreased compliance with relevant legislation or limitation of control possibilities; an on-site audit at the cloud-provider's premises may be

1 The CNB Decree 23/2014 implements certain requirements introduced by the CRD IV/CRR *(Directive of the European Parliament and of the Council on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms and Regulation (EU) No 575/2013 of the European Parliament and of the Council on prudential requirements for credit institutions and investment firms)*.

conducted by the regulatory authority in order to control the compliance of the financial institution with the relevant laws. Rules of control of the outsourcing provider's activities by the financial institution must be established. The legal relationships between the financial institution and its clients must not be affected by the outsourcing.

Annex 7 to the CNB Decree 23/2014 then provides further details about the requirements applicable to outsourcing including the requirements for a contract between the financial institution and the cloud provider. These include, for example, rules concerning designation of competencies, SLAs, threat notification, on-site audit rights, remedial measures, portability, subcontracting, or choice of law.

10

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

Yes. Pursuant to the CNB Decree 23/2014, a notification to CNB is required if a financial institution subject to its supervision deploys outsourcing regarding its "substantial activities" (defined as 'activities the failure of which would have significant impact on the capacity of the institution to fulfill security requirements or to perform its activities uninterruptedly, or activities the provision of which is conditioned by acquiring a public authorization to do so'). The notifying financial institution must inform CNB of the scope of outsourced functions and provide basic information about the outsourcing provider. Furthermore, the financial institution must inform CNB of any substantive changes regarding the outsourcing. These rules apply also to local branches of foreign financial institutions.

Cloud computing service provided by an external provider will be, in all likelihood, always considered outsourcing. While the notification requirement does necessarily not apply to all cloud computing services, it is nevertheless likely that in most cases the deployment of a cloud computing solution will amount to 'outsourcing of substantial activities' as defined above and will thus need to be notified. The applicability of the notification requirement should be assessed taking into account the specific circumstances of each outsourcing (cloud computing) arrangement.

The notification is not subject to any fees.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

Yes. Please see:

DPA's Opinion on legal protection of personal data in relation to their transfer within cloud services from August 7, 2013 (available in Czech only at http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002 on the DPA's website);

DPA's Opinion on whether cloud computing may be used for processing of personal data from April 2, 2013 (available in Czech only at the DPA's website http://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=1655&n=lze-vyuzit-cloud-computing-pro-zpracovani-osobnich-udaju&query=cloud)

PENDING LEGISLATION

14

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

New cyber security legislation is anticipated to be enacted and come to force in 2015. The current draft law includes, for example, an obligation of public bodies to implement, in case of cyber attacks, contingency plans for individual systems they operate in their "critical infrastructure", mechanism for identification of cyber attacks and for restoration of information, etc. While the proposed legislation does not deal directly with cloud computing, it might have some impact on the deployment of cloud by public sector bodies.

In a longer term, specific legal regulations may be adopted as a result of the implementation of the currently discussed e-Government policy[2] which calls, *inter alia*, for shared information society services, the adoption of which would entail the interconnection of certain public administration data resources, the setting and systematic application of standards for data interoperability, provision of information services and secure sharing of data, and the adoption of secured and verified electronic identification, authentication and authorization.

2 Document "*Strategický rámec rozvoje eGovernmentu 2014+" ("Strategic Framework of eGovernment Development 2014+")* submitted by the Ministry of Interior to the Czech Government in January 2014.

ESTONIA

COUNSEL DETAILS:

Country: Estonia
Attorney: Hannes Vallikivi
Law Firm: Tark Grunte Sutkiene
Roosikrantsi 2
10119 Tallinn
Estonia
Website: www.tarkgruntesutkiene.com
E-mail: estonia@tgslegal.com

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?

Personal Data Protection Act1 of 2007 (in Estonian, *Isikuandmete kaitse seadus*; hereinafter the "Privacy Act"). The Privacy Act follows the rules set out by the EU Data Protection Directive, but is not identical with it.

The English version of the Privacy Act is available online at https://www.riigiteataja.ee/en/eli/512112013011/consolide.

2

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

Andmekaitse Inspektsioon (the "Data Protection Inspectorate", hereinafter **DPA**).

Address: 19 Väike-Ameerika St., 10129 Tallinn, Estonia. The DPA can be contacted through their website, available at http://www.aki.ee/en or directly through e-mail: info@aki.ee.

The DPA is a supervisory authority referred to in Article 28 of the EU Data Protection Directive. It monitors compliance with the Privacy Act and legislation established on the basis thereof. In addition, the DPA is a supervisory authority for freedom of information matters (Public Information Act) and for direct e-marketing (Electronic Communications Act). The DPA is a governmental authority under the Ministry of Justice and has the typical powers of executive authority (investigations which may include coercive measures, precepts, substitutive enforcement, misdemeanor and coercive fines and enforcement proceedings without court decision).

The DPA only has supervisory authority over cloud customers and cloud providers located in the territory of the Republic of Estonia. However, the DPA has also used non-governmental measures (e.g. sent letters to cloud providers located outside of the territory of Estonia and if necessary, contacted the DPA of the respective country) to protect the privacy rights of Estonian citizens. The DPA has authority over data processing that occurs on the territory of Estonia even if the cloud customer is located outside of Estonia (unless the data is merely transmitted through the territory of the European Union).

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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. Requirements with respect to processing sensitive personal data go beyond the requirements of the EU Data Protection Directive (please see question 8).

With respect to data processing and data processing agreements, the Privacy Act follows the requirements of the EU Data Protection Directive and does not go beyond its requirements.

5

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

As a general principle, the Privacy Act requires that data processors use technical and organizational measures to guarantee the safety of the data. The Privacy Act further lists measures that are mandatory and that include:

(i) Restricting access rights solely to authorized personnel and implementing measures that prevent unauthorized access to data processing equipment and other unauthorized operations

(ii) Keeping log entries (information who and when accessed which data) as well as information to whom data were transmitted.

(iii) Organizing work flow in the processor's enterprise, agencies or organizations in a manner that allows compliance with data protection requirements.

(iv) Keeping account of the equipment and software under the processor's control used for processing of personal data, and recording the name, type, location and contact details of the producer of the equipment and software and the name and version of the software.

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. DPA's approval is obligatory even in cases where the data transfer is based on EU Standard Contractual Clauses or Safe Harbor. This is because the law presumes that sufficient level of protection is guaranteed only in the EU and the EEA and in countries whose level of protection has been evaluated as sufficient by the European Commission.

The approval procedure usually takes up to 30 days, but the DPA may extend it up to 60 days. The chief processor must guarantee in the application for approval that the rights and inviolability of the private life of the data subject in the third country in the specific case is protected. The approval process is free of charge.

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.

A specific transfer regime applies to transfer of personal data obtained or created in the process of performance of public duties. In deviation of the EU Data Protection Directive Article 26(1)(f) which allows, by way of an exception, for a transfer to third countries of personal data contained in a public register, the Privacy Act extends this exception to 'any personal data obtained or created in the process of performance of public duties' (as long as these do not contain any sensitive personal data or as long as access to such data has not been restricted for any other reasons), i.e. the exception is broader as it does not apply solely to data kept in specific public registers.

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 following specific local law requirements apply:

The processing of sensitive personal data has to be registered with the DPA or the data controller/processor must appoint a person responsible for the protection of personal data within its organization. Such appointed privacy officer is independent in his or her activities from the data controller/processor and must monitor the compliance of the data controller/processor's processing operations with the Privacy Act.

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.

Internal rules and regulations must be established for any outsourcing (including IT outsourcing) activities. The Financial Supervisory Authority recommends that the supervisory boards of the financial institutions establish strategic general principles for outsourcing. The recommendation is available online at http://www.fi.ee/failid/Nouded_finantsjarelevalve_subjekti_poolt_tegevuse_edasiandmisele_outsourcing_v6.pdf (only in Estonian).

Financial institutions must conduct a thorough risk analysis before resorting to outsourcing. Outsourcing must not hinder the economic activities of the financial institution, the interests of clients or the conduct of supervisory activities of both the Financial Supervisory Authority and the financial institution over the provider. The financial institution must conduct a thorough audit of the service provider; it must ensure that the provider possesses the necessary qualifications, is able to ensure the sustainability of operations, and evaluate all risks relating to cross-border outsourcing.

Further requirements are stipulated as to the contents and scope of the

outsourcing contract (including the ownership of intellectual property, safety, etc.) as well as the continued compliance with relevant legislation and supervisory possibilities.

Under the current Credit Institutions Act, data relating to the data of specific clients and data which enable to ascertain the identities of specific clients are considered banking secret (even in encrypted form). This regulation is subject to change in the near future (please see response to question 11).

Client details subject to banking secrecy may currently be disclosed by a credit institution to a third party only with the written consent of the client.

10

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

No, approval or notification of regulatory authorities is not required.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

Yes, in April 2014 the DPA issued a general guidance outlining the main issues, benefits and risks associated with cloud computing, which is available only in Estonian at the DPA's website http://www.aki.ee/et/pilvandmetootlus.

PENDING LEGISLATION

14

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

Yes, an amendment to the Credit Institutions Act is pending promulgation by the President under which data that does not enable to ascertain the data of single clients or the identity of persons (e.g. encrypted data) shall no longer be considered banking secret. This amendment is specifically designed to allow banks a more extensive access to cloud computing services.

As the Credit Institutions Act permits the inclusion of a data subject's consent with processing of his/her personal data in the standard terms of the service provider, it may be anticipated that once the bank secrecy regulation is amended, this will facilitate the adoption of cloud computing services by financial institutions.

GREECE

COUNSEL DETAILS:

Country: Greece
Attorney: Takis Kakouris
Law Firm: Zepos & Yannopoulos
75 Katehaki & Kifissias Ave.
115 25 Athens
Greece
Website: www.zeya.com
E-mail: t.kakouris@zeya.com

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?

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data, as amended (the "Privacy Act"). The Privacy Act is substantially identical with and constitutes the implementation of the EU Data Protection Directive into Greek law. For an English version of the Privacy Act please visit

http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2013-EN.PDF.

In addition, Law 3471/1997 on the Protection of personal data and privacy in the electronic communications sector constitutes an implementation of Directive 2002/58/EC.

2

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

Data Protection Authority Offices: Kifissias 1-3, 115 23 Athens, Greece, tel: +30 210 6475600 website: www.dpa.gr, email: contact@dpa.gr

The DPA is a constitutionally consolidated independent authority, established by the Privacy Act. The main mission of the DPA is the protection of the personal data and the privacy of individuals in Greece from the unlawful processing of their personal data and their assistance in case it is established that their rights have been violated in any sector in accordance with the provisions of Law 2472/97 and 3471/2006.

The DPA has also the power to issue regulatory decision and guidelines, to issue permits for data collection and processing, to impose administrative sanctions set forth by the Privacy Act, to issue an annual report on its activities, to receive and respond to data protection related complaints and to perform investigations (including on-site investigations). Furthermore, the DPA maintains register of personal data processing operations and provides consultations in the area of personal data protection.

Generally, the DPA has only authority over cloud customers and cloud providers located in the territory of Greece. The DPA shall also have authority over data processing that occurs in Greece even if the data controller – cloud customer is established outside the territory of the EU (e.g. in the USA) but carries out processing in Greece through a Greek data processor – cloud provider (unless where it is merely a transit through Greece).

3

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

The Privacy Act provides for the same requirements as the ones reflected in question 2 in the EU Data Privacy Law section.

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?

Generally, there are no specific requirements going beyond the EU Data Protection Directive; the Privacy Act, however, provides a greater level of detail with respect to some of the requirements of the EU Data Protection Directive.

The Privacy Act explicitly provides for a joint and several liability of the data processor (cloud provider) and data controller (cloud customer) in certain circumstances. If a data processor discovers that the data controller is in breach of its statutory obligations, the data processor is obliged to notify the data controller thereof and terminate the processing immediately; otherwise, it becomes jointly and severally liable for damage caused to data subjects.

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: the scope and purpose of the processing, the term of the processing and contractual safeguards of the data processor (cloud provider) regarding technical and organizational security of the personal data and the joint and several liability of processor and controller towards the data subject.

The data processing operation between the data controller and data processor requires a simple notification to the DPA if the processor is Safe Harbor certified (US entities) or is in a country affording an adequate level of protection or the agreement follows the EU Standard Contractual Clauses. Otherwise, the data controller needs to obtain a permit from the DPA for the data processing operation.

5

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

The Privacy Act is technologically neutral and as such does not list specific measures, however, the DPA as per the authorization of the Privacy Act may and has issued guidelines and regulatory decisions setting forth specific requirements for the level of security of data and of the computer and information infrastructure, the security measures that are required for each category and type of data processing as well as the use of privacy-enhancing technologies.

In addition, the standardized notification forms through which data controllers notify the DPA about intended personal data processing (and that is available in an electronic form on the DPA's website) include a list of measures from which the notifying controller may choose to tick those that it had implemented in its organization (IT topology, code of conduct, security policy etc.)

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. Data transfers outside the EEA, even if based on EU Standard Contractual Clauses or EU-US Safe Harbor Framework, require a notification to the DPA. No permit/approval from the DPA is required.

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 such further requirements.

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?

No. Local law requirements for sensitive data reflect the provisions of the EU Data Protection Directive.

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.

Act of the Governor of the Bank of Greece ('BoG") no. 2577/2006 and in particular its Annex A (which was replaced by Annex 1 of Governor's Act no. 2597/2007) regulates outsourcing issues in the financial sector. Moreover, Act of the Governor of the BoG no. 33/19.12.2013 regulates outsourcing by Electronic Money Institutions. In the absence of a more specific regulation on cloud computing, the above Acts apply also on cloud computing which is generally accepted to be a form of outsourcing.

The BoG, management and the IT department of the financial institutions have the overall responsibility for the outsourcing policy and must implement an outsourcing policy document which should address, among other things, the scope of activities eligible for outsourcing, risk assessment and mechanisms deployed to mitigate the risks, provider selection procedures, archiving rules and a disaster recovery plan.

An outsourcing agreement between the financial institution and the outsourcing (cloud) provider must guarantee free access of the financial institution and its internal or external auditors to the financial statements, auditors' reports or any other relevant information concerning the outsourced activities as well as the access of the BoG to the financial data concerning the outsourced activity and the right of the BoG to conduct on-site audits. Such agreement must also include

clauses on the ramifications from breaches thereof, on the protection of confidential data of the institutions or their clients, on the internal control procedures, on disaster recovery plans as well as on other risk management measures which the provider is obliged to put in place. The agreement must also provide for the mechanism of settlement of disputes and for the obligation of the provider to notify the financial institution timely about any development that may materially impair its ability to carry out the outsourced activities.

10

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

Yes. If the outsourced operation qualifies as material or significant, the financial institution must receive a prior permit from the BoG.

An operation will be deemed to be material or significant if any defective or inadequate performance or omission thereof would materially impair the ongoing compliance of the financial institution with its operation license and the banking laws or its financial results or the continuity of the services provided. Except for core banking services, material or significant operations are operations of Internal Audit, Risk Management, Regulatory Compliance and central IT systems.

A permit will not be required even for material or significant operations, if the cloud provider is a credit or financial institution or investment firm licensed in Greece or in EEA or, if licensed outside the EEA, is subject to an equivalent level of regulatory supervision (in the latter case the financial institution must notify the BoG and a two-month deadline must then lapse).

If the operations are not material, the credit institutions must still inform the BoG in writing 30 days before the date of execution any the outsourcing agreement.

The approval and notification processes are not subject to any fees.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No. The DPA would in principle, rely on the guidance issued by WP 29 and other the EU institutions as outlined in response to question 14 of the EU Data Privacy Law section.

PENDING LEGISLATION

14

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

No.

HUNGARY

COUNSEL DETAILS:

Country: Hungary
Attorney: Dóra Petrányi, Márton Domokos
Law Firm: CMS Cameron McKenna LLP
H-1053 Budapest
Károlyi utca 12.
Hungary
Website: www.cms-cmck.com
E-mail: communications@cms-cmck.com

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 CXII of 2011 on the Right of Self-Determination in Respect of Information and the Freedom of Information (the 'Privacy Act'). The Privacy Act is substantially identical with the EU Data Protection Directive, with a few exceptions (e.g. definition of data processor, no recognition of Binding Corporate Rules, definition of processing for the purposes of legitimate interests). The Privacy Act can be found at the following link: www.naih.hu/files/Infotv-_MO.pdf.

2

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

Hungarian Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság – hereinafter referred to only as 'DPA). Its website can be found at www.naih.hu.

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C

The DPA is an independent central administrative body empowered to oversee compliance with the Privacy Act. The DPA is entitled to perform investigations (including on-site investigations), to issue decisions on administrative offences under the Privacy Act, and to impose fines and other measures for its violations. DPA receives complaints regarding alleged violations of the Privacy Act and responds to them. Furthermore, the DPA maintains register of personal data processing operations and provides consultations in the area of personal data protection. Generally, the DPA will only have authority over cloud customers and cloud providers located in the territory of Hungary. The DPA will have authority over data processing that occurs on the territory of Hungary even if the data controller – cloud customer is established outside the territory of the EU (e.g. in the USA) but carries out processing on the territory of Hungary.

Considering its practice (namely, one decision against a company in Slovakia) and its notes in its 2013 Annual Report, it appears that the DPA attempts to interpret the scope of the Privacy Act extensively, i.e. in a way to enable it to supervise those service providers that are located abroad but perform data processing operation pertaining to products or services provided to natural persons located in Hungary. The legal validity of such extensive interpretation was not yet confirmed by the legislator or any court where a decision of the DPA was appealed.

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section, with one exception. The Privacy Act applies to all data processing operations performed in Hungary that involve personal data.

Hungarian law applies to data processing carried out in Hungary even if it takes place in the context of the activities of a foreign data controller. This approach is stricter than Article 4 of the EU Data Protection Directive and Opinion 8/2010 on the applicable law of the WP 29.

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 Privacy Act explicitly provides for the following, rather strict liability of the data controller (cloud customer): data controllers shall be liable for any damage caused to a data subject as a result of unlawful processing or by any breach of data security requirements. The data controller shall also be liable for any damage caused by a data processor (e.g. cloud provider) acting on its behalf. The data controller may only be exempted from its liability if it proves that the damage was caused by reasons beyond its control.

The DPA 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. The Privacy Act does not prescribe the minimum content requirements of such agreements. However, the DPA recommends that data processing agreements contain at least (i) description of the specific activities of the parties, their decision-making rights and limitations, (ii) the possibility for the data controller to conduct security inspections, and the related formal requirements/documentation (origin, purpose of preparation, defining liability and tasks in the event of remedying shortcomings, etc.), (iii) detailed cooperation obligation especially in the event of data security incidents or data theft (e.g. crisis management, remediation, prevention of the occurrence of further losses, defining exact deadlines), (iv) data retention/deletion obligations and (v) "surviving obligations" after the termination of the data processing relationship.

The following data controllers and processors must appoint an internal data privacy officer who must hold a law degree, a degree in economics or information technology or an equivalent higher education degree and who reports directly to the head of the organization:

(a) data controllers or processors processing nation-wide jurisdictional, employment and criminal records;

(b) financial institutions; and

(c) electronic communications service providers and public utility services providers.

Otherwise, the appointment of internal data privacy officers is voluntary. The so-called 'conference of internal data privacy officers' provides for professional liaison between internal data privacy officers and the DPA on a regular basis.

5

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

In addition to the requirements set forth in Section VIII of the EU Data Protection Directive, the Privacy Act requires that personal data are protected against becoming inaccessible due to 'changes in the technology applied'. In order to protect data processed in various databases it must be ensured with adequate technical devices that the data stored in databases cannot, unless permitted by law, directly be linked to each other and traced back to the relevant persons.

Additional security measures and safeguards are specified for automated personal data processing. The Privacy Act does not specify any particular way to perform the above general obligations (e.g. to use a specific technology). In determining the measures to ensure security of processing, data controllers and processors shall proceed taking into account the latest technical development and the state of the art of their implementation. The DPA's publicly available investigations serve as a guideline for the assessment of the appropriateness of the technical and organizational measures: when reviewing such measures

of the data controllers, the DPA particularly checks the procedures regarding the exercise of access rights, the logging of data requests and the registration of data processing.

Personal data shall be protected against natural disasters, failures in the technology, human errors (intentional data breach, negligence, omission). Internal registers shall be kept separately. Unlawful entry of personal data shall be prevented, and data transfers and data recordings shall be traceable (logging). In case of any malfunctions, data recovery shall be available and all data accesses and errors shall be documented. Back-up copies shall be kept and security incidents shall be reported for internal analysis.

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?

No. Formal approval from / notification to the DPA is not required.

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.

Binding Corporate Rules are not recognized in Hungary

There are additional restrictions under Act L of 2013 on the Electronic Information Security of Governmental and Local Governmental Bodies: data processing by or done for a broad array of governmental bodies (including most authorities, ministries, security forces and municipalities) may be conducted solely in the territory of Hungary, or in a closed IT system maintained for diplomatic purposes, unless (i) the supervising

body or an international agreement allows it; and (ii) the data processing takes place in the territory of the EU. Data processing in relation to military operated governmental electronic information systems of European or national critical infrastructures (as defined by law) is possible without the approval of the supervising body or an international agreement, if it is performed in other EU countries.

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?

No. The rules and requirements largely mirror the provisions of the EU Data Protection Directive. Generally, a written consent is required for processing sensitive personal data (unless the data processing is required by law); however, the DPA also recognizes consent provided electronically if the data subject is unambiguously identifiable.

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.

4/2012 Management Circular of the Hungarian Financial Supervisory Authority (PSZÁF – its legal successor is the Hungarian National Bank, together: "HFSA") of 18 July 2012 on the Risks Resulting from the Use of the Community and Public Cloud Computing Services at Financial Institutions declares the engagement of cloud computing services as outsourcing, independently from the exact nature of the cloud service. As a result, compliance with the mandatory legal provisions of Act CCXXXVII of 2013 on Financial Institutions and Financial Enterprises on outsourcing shall be ensured, including certain mandatory terms of the cloud services (outsourcing) agreement. The outsourcing (cloud) agreement shall include the following key terms:

(i) Clear definition of the scope of the outsourced activities and data protection measures.

(ii) On-site and off-site audit rights of the financial institution, its internal and external auditor and the HSFA. In case of any breach of law / the cloud services agreement, the financial institution shall have the right to notify the HFSA.

(iii) Approval of any subcontracting (sub-processing) by the financial institution, and flow-down of audit rights for the HFSA, the financial institution and its internal and external auditors.

(iv) An obligation of the cloud provider to perform the cloud services with due care and extraordinary termination right for the financial institution in case of a serious or repeated breach of the cloud services agreement by the cloud provider.

(v) Detailed parameters on the quality of the cloud services (SLA).

(vi) Flow-down of mandatory legal provisions prohibiting insider trading.

(vii) "Conflict of interest provisions", i.e. the obligation to separate the customer data from data of other customers if the cloud provider is engaged by more than one client

The financial institution has an obligation to identify the cloud provider in its general terms and conditions.

Substantially similar obligations are applicable to insurance companies and investment service providers under the relevant sector-specific laws.

10

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

Yes. The financial institution shall notify the HFSA within 2 days of signing the outsourcing (cloud) services agreement of (i) the fact of the outsourcing; (ii) the name and address of the cloud provider; and (iii) the term of the outsourcing. Substantially similar obligations are applicable to insurance companies and investment service providers.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

Yes. Please see 4/2012 Management Circular of the Hungarian Financial Supervisory Authority (*PSZÁF*) of 18 July 2012 on the Risks Resulting from the Use of the Community and Public Cloud Computing Services at Financial Institutions (available in Hungarian only at the website of the Hungarian National Bank – legal successor of the HFSA - http://felugyelet.mnb.hu/data/cms2364896/vezkorlev_4_2012.pdf).

The DPA has so far provided little guidance on the implications of cloud computing under the Privacy Act. In its 2012 annual report, the DPA emphasized that it relied on the Cloud Opinion and on the Sopot Memorandum, and that the storage of "sensitive personal data" in the cloud was not recommended (but not prohibited). The 2012 Annual Report is available in Hungarian only on the website of the DPA - http://www.naih.hu/files/NAIH-2012-Beszamoloja-vegleges-web.pdf.

PENDING LEGISLATION

14

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

No.

LATVIA

COUNSEL DETAILS:

Country: Latvia
Attorney: Vineta Čukste
Law Firm: Kronbergs & Čukste Attorneys At Law
Muitas iela 1
Riga, LV-1010
Latvia
Website: www.blslawfirm.com/bls-latvia/home
E-mail: Advocate@lv.blslawfirm.com

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?

Personal Data Protection Law Regulations of the Cabinet of Ministers No. 634 of 16 August 2011 "Regulations on Compulsory Provisions of Personal Data Transfer Agreements" (the "Regulations 634").

Regulations of Cabinet of Ministers No. 40 of 30 January 2001 "Compulsory Technical and Organizational Measures of Personal Data Protection" (the "Regulations 40").

2

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

Datu valsts inspekcija (Data State Inspectorate, hereinafter referred to only as "DPA"), Blaumaņa iela 11/3-15, Riga, LV-1011, Latvia, tel. +371-67223131, fax: +371-67223556, email: info@dvi.gov.lv, web page: www.dvi.gov.lv.

The DPA is a state administration institution which is subject to supervision by the Ministry of Justice, and which performs supervision of protection of personal data, takes decisions and issues administrative acts in accordance with the Privacy Act. The duties of the DPA include taking of decisions and reviewing of complaints regarding the protection of personal data, registration of personal data processing systems, issuance of opinions regarding conformity of personal data processing systems to the regulatory requirements, accreditation of persons who wish to perform system audits of state and local government institution personal data processing systems etc.

The DPA is entitled to carry out necessary inspections and audits (including on-site audits) and impose other measures in order to determine the compliance of the personal data processing procedures with the Privacy Act.

Generally, the DPA will only have authority over cloud customers and cloud providers located within the territory of Latvia. The DPA will have authority over data processing that occurs on the territory of Latvia even if the data controller – cloud customer, is established outside the territory of the EU but carries out data processing on the territory of Latvia through a local Latvia – based data processor – cloud provider (unless it is merely transiting through the territory of the European Union).

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in our response to question 2 in the EU Data Privacy Law section.

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?

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 by prescribing the following minimum content requirements: the agreement must be in the Latvian language (or in a number of languages, one of which is Latvian). It must set out the scope and purpose of the processing, contractual safeguards of the data processor (cloud provider) regarding technical and organizational security of personal data, the obligations of data processor (cloud provider), the obligations of the data processor (cloud provider) to compensate damages, if any, caused by it to data subjects.

There are no other specific requirements going beyond the EU Data Protection Directive.

Certain requirements are, however, stipulated in more detail. For example, in line with the EU Data Protection Directive, the Privacy Act requires the data controller to register a personal data processing operation (and any amendments thereto) with the DPA, especially if personal data is intended to be transferred to third countries. However, this registration requirement does not apply if the data controller has appointed a data protection officer in its organization and has registered such person with the DPA.

5

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

The Privacy Act and Regulation 40 provides that technical protection of personal data must be ensured by physical and logical protection measures which safeguard personal data from physical influences and by software protection measures, passwords, encoding, encrypting, etc..

The data controller is required to ensure, inter alia, by drawing up internal regulations on data processing, that only authorised persons

have access to technical resources which are used for processing and protection of personal data; to register, relocate, put into order, transfer, copy and otherwise process information devices containing personal data; and that collection, recording, putting into order, storage, copying, re-recording, amending, deleting, destroying, archiving and blocking of personal data may only be performed by respectively authorised persons.

The data controller must also ensure that it is possible to identify personal data which was processed without the required authorisation, as well as the time of such processing and person who performed such processing.

Moreover, data controller must ensure that upon transfer and receipt of personal data, the following information is maintained: the time of transfer of personal data, the identity of the person who transferred personal data, the identity of the person who received the personal data, and the personal data which was transferred.

The data controller must perform annual internal audits of personal data processing and must inform persons who process personal data (including cloud providers) on these technical and organizational measures.

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. As already noted in the answer to question 4, the Privacy Act requires the data controller to register a personal data processing agreement (and any amendments thereto) with the DPA, particularly if personal data is intended to be transferred to third countries. However, this registration requirement does not apply if the data controller has appointed a data protection officer in its organization and has registered him with the DPA.

These requirements apply even if the transfer is based on EU Standard Contractual Clauses or EU-US Safe Harbor Framework.

In order to perform registration, a data controller must submit to the DPA a registration application (pre-print form) which contains the following information: name and registration number of the data controller and data processor, the legal basis of personal data processing, types of personal data and the objective of its processing, categories of data subjects, categories of recipients of personal data, planned manner of personal data processing, planned manner of obtaining of personal data, place of personal data processing, the holder of information and technical resources and the person responsible for information system safety, technical and organizational measures ensuring protection of personal data.

The DPA is to perform registration within 30 days after receipt of an application, and if the DPA finds any shortcomings in the application, they must be corrected within 30 days.

The data controller must pay a stamp duty in the amount of 50 Euro for the aforesaid registration.

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.

Please see the above answer to question 6 regarding registration with the DPA of any data processing agreements, in particular where the processor is based in a third country.

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?

No. The rules and requirements largely mirror the provisions of the EU Data Protection Directive.

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.

Law on Credit Institutions permits outsourcing of services of credit institutions related to management and development of information technologies and systems. Such outsourcing may only be made to service providers with sufficient qualifications and experience, and must not result in decreased compliance with applicable legislation or limitation of control possibilities. An on-site audit at the cloud provider's premises may be conducted by the regulatory authority (the Latvian Financial and Capital Market Commission) in order to verify compliance of the financial institution with applicable law. In addition to the audit rights of the regulator, rules of control of the outsourcing provider's activities by the financial institution must be established. The legal relationship between the credit institution and its clients may not be affected by the outsourcing and the credit institution continues to be fully liable towards its clients.

There exists no official DPA guidance on this matter.

10

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

Prior to subcontracting of any services, a credit institution must submit a written notification to the Latvian Financial and Capital Market Commission by attaching subcontracting policies, a description of procedures and the signed subcontracting agreement. The subcontracted party may start providing services if the Latvian Financial and Capital Market Commission has not issued a prohibition regarding same within 30 days after receipt of written notification. The notification is not subject to any fees.

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 for a cloud provider to mine customer data for advertising purposes. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No. There is no specific guidance on cloud computing issued by the DPA.

However, the DPA's Guidelines of Transfer of Personal Data to Third Parties also apply to cloud computing: (available in Latvian only at http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Rekomendacija_3_valstis.pdf on the DPA's website.

PENDING LEGISLATION

14

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

No. The new Cyber Safety Strategy for the years 2014-2018 might result in some legislative changes possibly also affecting cloud computing but no specific draft laws have yet been produced.

LITHUANIA

COUNSEL DETAILS:

Country: Lithuania
Attorney: Iraida Žogaitė, Paulius Zapolskis
Law Firm: Baltic Legal Solutions Lithuania
Subačiaus st. 7
Vilnius
Lithuania
Website: www.blslawfirm.com/bls-lithuania/home
E-mail: lithuania@blslawfirm.com

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?

Law No. I-1374 on Legal Protection of Personal Data of the Republic of Lithuania (the "Privacy Act"). The Privacy Act is substantially identical with the EU Data Protection Directive. English version of the Privacy Act is available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=435305.

The following local legal acts could also be relevant for cloud computing – Resolution No. 262 of the Government of the Republic of Lithuania on the Approval of the Regulations of the Register and of the Procedure of Notification by Personal Data Controllers of Automated Processing of Personal Data; Order No. 1T-71(1.12) of the Director of State Date Protection Inspectorate on the Approval of General Organizational and Technical Measures of Data Security (hereinafter referred to as the

"Data Security Order"). English version of the Data Security Order is available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=331500&p_query=&p_tr2= .

2

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

Valstybinė duomenų apsaugos inspekcija ("State data protection inspectorate", hereinafter referred to only as "DPA")

Address: A. Juozapavičiaus str. 6, 09310 Vilnius, Lithuania, e-mail ada@ada.lt, website https://www.ada.lt.

The DPA is an independent central administrative body empowered to oversee compliance with the Privacy Act. The DPA administers the State Register of Personal Data Controllers, supervises the activities of data controllers relating to the processing of personal data, examines complaints and notifications by persons, checks the lawfulness of personal data processing based on these complaints and takes decisions concerning violations in personal data processing etc.

Generally, the DPA will only have authority over cloud customers and cloud providers located in the territory of the Republic of Lithuania. The DPA will have authority over data processing that occurs on the territory of the Republic of Lithuania even if the data controller – cloud customer is established outside the territory of the EU (e.g. in the USA) but carries out processing on the territory of the Republic of Lithuania through a local (Lithuanian-based) data processor – cloud provider (unless where it is merely a transit through the territory of the European Union).

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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 liability rules established in the Privacy Act go beyond the requirements of the EU Data Protection Directive and imposes liability not only upon the data controller but also upon the data processor and the third parties who are infringing the Privacy Act. The Privacy Act establishes that any person who has sustained damage as a result of unlawful processing of personal data or any other acts (omissions) by the data controller, the data processor or other persons violating the provisions of the Privacy Act, shall be entitled to claim compensation for incurred pecuniary and non-pecuniary damage.

The Privacy Act also prescribes that the organizational and technical measures implemented by the data controller and the data processor must be defined in a written document (personal data processing regulations approved by the data controller, an agreement concluded by the data controller and the data processor, etc.). The specific requirements for the contents of the personal data processing regulations or an agreement concluded by the data controller and the data processor are established in the Data Security Order, which elaborates, in a great level of detail, on the general provisions of the EU Data Protection Directive.

The Privacy Act explicitly regulates two fields that are not directly covered by the EU Data Protection Directive, namely, processing of personal data for the purpose of video surveillance and processing of personal data for the purpose of evaluation of solvency and debt management. The Privacy Act also establishes requirements regarding form and content of notifications to data subjects which include personal data when sending such notification by post.

5

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

The Privacy Act is technologically neutral and as such does not list specific measures. The data controller must however indicate *inter alia* the applicable data security level depending on the type of data processed by that controller upon notification of the DPA about intended personal data processing (notification form is available in an electronic form on the DPA's website). The specific, detailed requirements for each security level, such as access rights, anti-virus protection, security backups, data encryption etc., are prescribed in the Data Security Order.

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. As already noted in the answer to question 4, the Privacy Act requires the data controller to register a personal data processing agreement (and any amendments thereto) with the DPA, particularly if personal data is intended to be transferred to third countries. However, this registration requirement does not apply if the data controller has appointed a data protection officer in its organization and has registered him with the DPA.

These requirements apply even if the transfer is based on EU Standard Contractual Clauses or EU-US Safe Harbor Framework.

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?

No.

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.

Resolution No. 149 of the Central Bank of the Republic of Lithuania (hereinafter referred to as the „CB") on Approval of the Rules on the Organization of the Internal Control and Risk Assessment (Management)[1] provides that in case financial institutions outsource any of the electronic data recording, transfer, processing and storage activities (i.e. including any outsourcing of IT functions, which would also cover cloud computing; see next question) these financial institutions must assess the associated strategic, organizational, legal and other types of risk. Furthermore, financial institutions must meet all the requirements established in the Resolution No. 99 of the CB on Approval of the Rules on Outsourcing Services Supplementing the Bank's Activities[2] (hereinafter referred to as the „Rules on Outsourcing"). According to the Rules on Outsourcing, prior to procuring the services the financial institutions must verify that the outsourcing provider is financially stable, competent, resourceful and able to provide quality and timely services.

1 The Lithuanian language version of the Resolution is available at https://www.e-tar.lt/portal/forms/legalAct.html?documentId=TAR.2E636440A883
2 The Lithuanian language version of the Resolution is available at https://www.e-tar.lt/portal/forms/legalAct.html?documentId=TAR.68A7DD416B3E

The Rules on Outsourcing also establish the mandatory requirements of an outsourcing contracts which include, inter alia, a clear definition of outsourced activities including qualitative requirements (service levels); parties' responsibilities; information obligations of the service provider towards both the financial institution and the CB; termination rights of the financial institution; confidentiality undertakings of the service provider; audit rights of the financial institution vis à vis the service providers and any subcontractors, and other obligations.

10

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

Yes. Pursuant to the Rules on Outsourcing, a notification to CB is required if a financial institution subject to its supervision deploys outsourcing regarding its "significant activities" (IT software programming and maintenance activities as well as maintenance of IT infrastructure are deemed "significant activities"). A notification must be submitted at least 30 days prior to concluding a contract with the outsourcing provider. Financial institution must inform the CB on the scope of outsourced functions, provide basic information about the outsourcing provider and provide the draft contract with the outsourcing provider meeting the requirements established in the Rules on Outsourcing. Furthermore, the financial institution must provide reasons of the decision to outsource the particular services instead of using internal resources.

Cloud computing services provided by an external provider will be, in all likelihood, always considered outsourcing. The applicability of the notification requirement should be assessed taking into account the specific circumstances of each outsourcing (cloud computing) arrangement.

The notification is not subject to any fees.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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. While the Privacy Act does not explicitly elaborate on the transparency requirement, generally, this principle as outlined in response to question 11 of the EU Data Privacy Law section applies.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No, there is no local guidance on cloud computing.

PENDING LEGISLATION

14

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

No. The DPA, however, considers adopting a cloud computing concept by the end of 2014.

MALTA

COUNSEL DETAILS:

Country: Malta

Attorney: Dr. Antoine Camilleri, Dr. Claude Micallef-Grimaud

Law Firm: Mamo TCV Advocates
Palazzo Pietro Stiges
103 Strait Street
Valletta VLT 1436
Malta

Website: www.mamotcv.com

E-mail: info@mamotcv.com

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?

The Data Protection Act (Chapter 440 of the Laws of Malta) and the Regulations (at present eight in number) issued under it ("Privacy Act"). The Privacy Act largely implements the European Data Protection Directive (Directive 95/46/EC) as well as the E-privacy Directive (2002/58/EC).

The above legislation is available at:

http://www.justiceservices.gov.mt/LOM.aspx?pageid=27&mode=chrono&gotoID=440

2

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

Office of the Information and Data Protection Commissioner ("DPA")

Airways House

Second Floor

High Street

Sliema SLM 1549

Malta

T +356 2328 7100

F +356 23287198

idpc.info@gov.mt

www.dataprotection.gov.mt

The DPA has the function (among other things) of generally ensuring the correct processing of personal data in order to protect individuals from violations of their privacy. The DPA has various powers including inter alia, to perform investigations (including on-site investigations), to issue various orders (including rectification and erasure of data), to impose fines and penalties as well as to take other measures in case of non-compliance with the provisions of the Privacy Act. The DPA receives complaints regarding alleged violations of the Privacy Act and responds to them (usually by way of an investigation). In addition, the DPA maintains a register of data controllers (and data protection representatives) as well as of notified processing operations. The DPA also offers consultations in the area of personal data protection and authorizes transfers of personal data to certain third countries.

Generally, the DPA will only have authority over processing of personal data carried out in the context of an establishment of a controller in the Republic of Malta or in cases of non-establishment in Malta (e.g. if the controller is established in the US) where the equipment used for processing personal data is situated in Malta – unless the said equipment is used only for purposes of transit of information between a third country and another such country.

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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?

The requirements of the EU Data Protection Directive generally apply.

5

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

The Privacy Act does not elaborate further on the phrase 'technical and organizational measures' and therefore this must generally be examined on a case-by-case basis.

The notification form through which data controllers notify the DPA about intended personal data processing (and that is available in an electronic form on the DPA's website) includes a list of measures from which the notifying controller may choose to tick those that it had implemented in its organization. This non-exhaustive list of measures includes the following:

(i) necessary data protection awareness and training;

(ii) a record of persons who access the system;

(iii) logins and passwords;

(iv) access rights/privileges,;

(v) audit trails and physical safeguards including locks (of offices, file cabinets, etc.).

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?

Transfers of personal data from Malta to any country that is not an EU Member State (i.e. to a 'Third Country' as defined under the Privacy Act) must always be *notified* by data controllers to the DPA (by means of an *ad hoc* data transfer form in addition to the general notification requirements).

Transfers of personal data to a Third Country are only permitted if the standard conditions for transborder data transfers as regulated by the EU Data Protection Directive ('Standard Conditions for Transborder Transfers') are satisfied. If a transfer does not satisfy these conditions, in addition to the requirement of notification, the transfer must also be approved by the DPA.

Transfers of personal data based on the EU Standard Contractual Clauses may require prior authorization from the DPA depending on the Third Country in question. If the said Third Country is an EEA country and/or an EU Commission-white-listed country (i.e. a country that the EU Commission has found to provide an adequate level of protection for personal data) then no prior authorization from the DPA is required (and only notification will be required).

Transfers of personal data to U.S. organizations complying with the EU-US Safe Harbor Framework require only notification to the DPA (no authorization is required).

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.

Specific *notification* to the DPA of transfers of data to Third Countries must always take place prior to the commencement of processing operations (even in those cases where the DPA's *approval* is not required). In those cases where the DPA's approval is required, evidence of compliance with the Standard Conditions for Transborder Transfers (such as sample consent forms and/or copies of relevant data processing agreements,

as applicable) must be included by way of annex together with the said (*ad hoc*) notification form. The form can be viewed at:

http://idpc.gov.mt/dbfile.aspx/International%20Data%20Transfer%20Form.pdf

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?

The requirements of the EU Data Protection Directive generally apply.

Data relating to offences, criminal convictions or security measures may only be processed under the control of a public authority and a complete register of criminal convictions may only be kept under the control of a public authority. Legal Notice 142 of 2004 and Legal Notice 198 of 2011 contain a set of more detailed regulations on the processing of personal data by police and judicial cooperation in criminal matters.

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.

There is no Maltese legislation dealing specifically with cloud computing (and no explicit DPA guidance on the matter). However, rules applicable to outsourcing will apply to (i) credit institutions (also referred to as banks) and (ii) other financial institutions (the main difference between these two being that the latter institutions are not allowed to take deposits or other repayable funds from the public). Both these categories are regulated separately (even though, in some cases certain overlap may exist between the two).

Relevant legislation regulating this matter includes the following:

(i) The Banking Act (Chapter 371 of the Laws of Malta), available at: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8840&l=1.

The Banking Act imposes a general restriction on the outsourcing: credit institutions licensed under the Banking Act are not allowed to outsource material services or activities unless the outsourcing service provider is granted recognition by the Malta Financial Services Authority (MFSA). The MFSA has certain supervisory powers to request information and documentation from and to investigate outsourcing service providers.

(ii) Banking Rule – Outsourcing by Credit Institutions authorised under the Banking Act (BR/14/2009) and issued by the MFSA, available at: http://www.mfsa.com.mt/pages/readfile.aspx?f=/files/LegislationRegulation/regulation/banking/creditInstitutions/rules/BR14-231209.pdf.

The Banking Rule applies to credit institutions licensed by the MFSA and lays down detailed rules on outsourcing. These rules also regulate, inter alia, the procedure for obtaining recognition as an 'outsourcing service provider'.

(iii) The Financial Institutions Act (Chapter 376 of the Laws of Malta), available at: http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8843&l=1.

It requires a financial institution that intends to outsource operational functions of its services or activities to obtain the recognition of the outsourcing service provider from the MFSA, and regulates outsourcing of "important operational functions" (which may include cloud computing services).

The MFSA has certain supervisory powers in relation to entities to which activities are outsourced, including the right to conduct on-site inspections.

(iv) Financial Institutions Rule – Supervisory and Regulatory Requirements of Institutions Authorized under the Financial

Institutions Act (FR/ 02/2011) issued by the MFSA, available at: http://www.mfsa.com.mt/pages/readfile.aspx?f=/Files/LegislationRegulation/regulation/banking/financialInstitutions/rules/20110712%20FIR%2002.pdf.

With respect to outsourcing, these regulations cross-refer to the Financial Institutions Act, the Banking Rule as well as the CEBS Guidelines on Outsourcing issued on 14 December 2006. Credit institutions as well as other financial institutions require an 'outsourcing service provider' to be recognized by the MFSA before outsourcing (by cloud clients to cloud service providers) can be undertaken.

In addition, the DPA issued the following guidance that is also relevant for data processing operations in the finance sector:

(i) Guidelines for the Promotion of Good Practice in the Banking Sector, available at: http://idpc.gov.mt/dbfile.aspx/Banking%20Guidelines.pdf.

(ii) Data Protection Guidelines for the promotion of good practice - Processing of personal data by Credit Referencing Institutions, available at: http://idpc.gov.mt/dbfile.aspx/CRA_Guidelines.pdf.

(iii) Guidelines for the Promotion of Good Practice – Insurance Business Sector, available at: http://idpc.gov.mt/dbfile.aspx/Insurance%20Guidelines.pdf

Outsourcing rules also apply in other areas of financial services regulation (e.g. investment services and collective investment schemes).

10

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

Yes. Outsourcing service providers deployed by credit institutions and other financial institutions need to be recognized by the MFSA before cloud services may be supplied by them. A written application for approval must be submitted to the MFSA. Non-complex cases will generally require a few weeks to obtain the necessary approvals. There are no administrative fees associated with the application for and issuance of the approval.

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. Certain specific exceptions apply to electronic marketing under the 'Processing of Personal Data (Electronic Communications Sector) Regulations 2003' (Legal Notice 16 of 2003 as amended) which regulates, inter alia, the use of electronic contact details for unsolicited communication.

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 key transparency requirements as outlined in response to question 11 of the EU Data Privacy Law section apply.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No. The DPA refers in its communication to the Cloud Opinion.

PENDING LEGISLATION

14

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

No.

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.

ROMANIA

COUNSEL DETAILS:

Country: Romania
Attorney: Andreea Lisievici
Law Firm: Țuca Zbârcea & Asociații
4-8 Nicolae Titulescu Ave., America House, West Wing, 8th Floor,
011141, Bucharest
Romania
Website: www.tuca.ro
E-mail: office@tuca.ro

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?

Law No. 677/2001 on the protection of persons concerning the processing of personal data and the free movement of such data (hereinafter the "Privacy Act"), published in the Official Gazette of Romania No. 790 dated 12 December 2001, as subsequently amended and supplemented. An unofficial translation into English of the Privacy Act, as well as of some related legal enactments may be found on the website of the DPA, at http://dataprotection.ro/index.jsp?page=legislatie_primara&lang=en.

The Privacy Act fully implements the EU Data Protection Directive, having substantially similar provisions. However, the Privacy Act also includes several provisions which are stricter than those under the EU Data Protection Directive, as discussed in the relevant sections below.

2

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

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (*The National Supervisory Authority For Personal Data Processing, hereinafter the "DPA"*).

Address: 28-30 G-ral Gheorghe Magheru Bld., 1st district, 010336 Bucharest, Romania

Website: http://dataprotection.ro

The DPA is an independent public authority legally entrusted with overseeing and controlling the legality of personal data processing falling under the scope of the Privacy Act. The DPA is the authority receiving notifications of personal data processing, issuing authorizations for such processing where such authorizations are required, and also investigating and sanctioning controllers and processors which fail to comply with the Privacy Act. The DPA also issues administrative regulations in the field of personal data processing, some of which are also translated into English at http://dataprotection.ro/index.jsp?page=publicated&lang=en.

The DPA is competent in matters involving cloud providers located in Romania, as well as cloud providers which are located abroad, but use any means located in Romania, except where such means are only used to transit personal data through Romania. The jurisdiction of the DPA does not account for "targeting", thus cloud providers located abroad, not using "any means" located in Romania but offering their services to Romanian cloud customers, fall outside of such jurisdiction.

3

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

The requirements for the applicability of the Privacy Act are similar to those under the EU Data Protection Directive as indicated in response to question 2 in the EU Data Privacy Law section. However, there is a certain discrepancy arising from the fact that, while the EU Data Protection Directive refers to "equipment" located within the EU, the Privacy Act refers to "any means" located in Romania. In the absence of an official interpretation by the DPA of what these "means" refer to, it

appears that the scope of application of the Privacy Act may be broader than that of the EU Data Protection Directive[1].

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?

The requirements for the applicability of the Privacy Act are similar to those under the EU Data Protection Directive as indicated in response to question 2 in the EU Data Privacy Law section. However, there may be a discrepancy arising from the fact that, while the EU Data Protection Directive refers to "equipment" located within the EU, the Privacy Act refers to "any means" located in Romania. In the absence of an official interpretation by the DPA of what these "means" refer to, it appears that the scope of application of the Privacy Act may be broader than that of the EU Data Protection Directive[2].

5

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

Order No. 52/2002 issued by the Ombudsman (which at that time was the DPA) setting forth the minimal security requirements for processing personal data. These minimal requirements are intended to ensure the confidentiality and integrity of personal data (privacy by design), and are meant to represent the foundation based on which controllers draft their own security policies and procedures, which must be attached to the personal data processing notification to the DPA.

The minimal security requirements concern the following main aspects:

(i) Each user[3] must be identified based on unique means (identification

1 For example, since it is questionable whether cookies stored in the customer's computer represent "equipment", they might be considered to fall within the meaning of "any means" located in Romania.
2 For example, although it is questionable whether cookies stored in the customer's computer represent "equipment", they might be considered to fall within the meaning of "any means" located in Romania.
3 "User" is defined as any person acting under the authority of the controller or the processor, having the right to access the databases of personal data.

code, barcode, smart card). Authentication is mandatory for accessing the system, and may be made by using passwords or biometric means, subject to certain minimal requirements.

(ii) Backup copies of the database must be made regularly, within the time frames required by the controller. The back-up copies must be stored in separate rooms or, if possible, separate buildings.

(iii) Access to personal data must be made only on a need-to-know basis. Access must be restricted either to the rooms or to each terminal (via passwords, access cards or similar). Working sessions must terminate automatically after a period of inactivity. The terminals used in public relations must be placed so as not to allow the public to have access to the personal data on the screen.

(iv) Any accessing and change of the database must be logged, by recording at least the data provided by Order no. 52/2002.

(v) In case of telecom systems, the controller must periodically check the functionality of the system, and to design it so as to ensure that personal data may not be intercepted or ensure encryption of the data.

(vi) Users must be trained concerning the data protection obligations provided by the Privacy Act, the applicable security requirements, and the risks entailed by the processing of personal data.

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. Under the Privacy Act, any transfer of personal data outside of Romania must be notified to the DPA. Where the destination country is outside of the EEA, has not been recognized as providing an adequate level of protection by the Commission, and is not subject to the EU-US Safe Harbor Framework, an authorization for the transfer is required. This includes the case of Standard Contractual Clauses being used, however

in such a case the authorization for transfer cannot be denied, as the DPA can only acknowledge that the use of the Standard Contractual Clauses ensures an adequate level of protection.

The procedure of filing the data processing notification and, if applicable, requesting the authorization is free of charge. Where only the notification is required, the controller may start the data processing within 5 days from filing the notification, provided the DPA does not notify within such time the need to perform a prior investigation.

If the data processing requires authorization, the Privacy Act and related documents do not provide a time limit within which the DPA must issue the authorization. In practice, the authorizations are issued in about two months from the moment when the DPA considers the notification and related documents to be complete.

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.

The transfer of personal data outside of the EEA will always require notification to the DPA. Where the destination country is outside of the EEA, has not been recognized as providing an adequate level of protection by the Commission, and is not subject to the EU-US Safe Harbor Framework, the DPA must authorize the transfer, including when the transfer relies on the EU Standard Contractual Clauses.

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 includes supplementary restrictions for processing identification data and medical data.

More specifically, the personal identification code[4] or other personal data

4 Pursuant to Romanian law, Romanian citizens as well as foreign residents or national residents have a unique personal identification code consisting of 13 digits, which is printed on the identification or residence documents.

having a general identification purpose (such as the passport number, driver's license number, social security number, etc.) may be processed only if the data subject had expressly consented, or if the processing is provided for under the law. DPA Decision no. 132/2011 further states that the processing of identification data may also be made in other situations, provided that the DPA endorses such processing and the controller ensures sufficient guarantees concerning the observance of the rights of data subjects.

The Privacy Act also provides that medical data may be processed by medical doctors, health centers and their medical staff without authorization from the DPA only if such processing is required to protect the life, physical integrity or health of the data subject. When medical doctors, health centers and their medical staff process medical data of other persons or the general public and the data subject has not given its express written consent, a prior authorization must be obtained from the DPA.

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 use of cloud computing by financial institutions may classify as outsourcing of activities, if the cloud services consist of activities previously carried out by the financial institution (e.g. electronic archiving, e-mailing services, etc.). Regulation No. 5/2013 issued by the National Bank of Romania on the prudence requirements for credit institutions[5] provides that activities may be outsourced subject to the prior approval of the National Bank only if this does not impact the activity of the credit institution which must comply with all applicable legal and regulatory requirements, the exercise of attributions by the management body of the credit institution or the prudential supervision of the credit institution by the National Bank of Romania.

5 Available in Romanian language at http://bnr.ro/apage.aspx?pid=404&actId=326618.

Regulation No. 5/2013 also includes specific requirements for the outsourcing agreement, most notably the following:

(i) The inclusion of a clause allowing the termination of the contract, if deemed necessary and proportionate to the outsourced activity, to enable the transfer of the activity to another external supplier or its re-inclusion into the credit institution;

(ii) The inclusion of provisions concerning the protection of confidential information, processing that information and keeping the banking secret by the external provider, at least at the same level as the credit institution;

(iii) Providing the obligation incumbent on the external supplier to allow, in connection to the outsourced services, the direct access of the National Bank to its data, as well as the performance by the National Bank of on-site inspections;

(iv) Providing the obligation incumbent on the external supplier to allow the bank's audit and compliance function access the complete data of the external provider, and the bank's financial auditor right to inspect and audit the data;

(v) Providing the obligation incumbent on the external supplier to obtain the approval of the credit institution before subcontracting parts of the services outsourced by the credit institution. Moreover, the regulation also provides that the credit institution may consent to such a chain outsourcing only in case the subcontractor undertakes the same obligations as those incumbent on the main external, including those in relation to the National Bank.

10

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

Yes. The outsourcing of "significant activities"[6] is subject to a prior notification to the National Bank of Romania, submitted at least two months prior to the conclusion of the outsourcing agreement.

While the notification requirement does not necessarily apply to all cloud computing services, it is nevertheless likely that in most cases the deployment of a cloud computing solution will amount to 'outsourcing of significant activities' and thus be subject to the obligation to notify the National Bank. While the National Bank cannot forbid the outsourcing, it may require the credit institution to take the actions or implement the measures prescribed by the National Bank.

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. The Privacy Act does not have special provisions in this respect, thus the general provisions implementing the purpose specification and limitation principle of the EU Data Protection Directive, as indicated in the response to question 10 of the EU Data Privacy Law section, shall apply.

6 Regulation No. 5/2013 defines "significant activities" as:
a) activities of such importance that any difficulty or failure in their development could have a material adverse effect on the credit institution's ability to fulfill its obligations under the regulatory framework and / or to continue their activity;
b) any other activities that require an authorization from the competent authorities;
c) any activities that have a significant impact in terms of risk management; and
d) risk management related to activities under letter a).

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 Privacy Act has no special provisions concerning cloud computing services, thus the same principles and requirements outlined in the response to question 11 of the EU Data Privacy Law section remain applicable.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No.

PENDING LEGISLATION

14

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

No.

SLOVAKIA

COUNSEL DETAILS:

Country: Slovakia
Attorney: Jana Pattynová
Law Firm: PIERSTONE s.r.o., advokátní kancelář
Na Příkopě 9
110 00 Prague 1
Czech Republic
Website: www.pierstone.com
E-mail: jana.pattynova@pierstone.com

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 no. 122/2013 Coll., Act on personal data protection and on amendment and supplement of other laws, as amended (the "Privacy Act"). The English version of the Privacy Act will be soon available at http://www.dataprotection.gov.sk.

The Privacy Act is substantially identical with the EU Data Protection Directive; it provides for several additional obligations for data controllers and data processors and stipulates some obligations in more detail. The current Privacy Act has only been effective since 1 July 2013 and, as a result of a strong opposition from the private sector against certain provisions, it has been recently amended (effective as of 15 April 2014). Some of the changes introduced by the amendment will have impact on cloud computing (for details, see below the responses to individual questions).

2

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

Úrad na ochranu osobných údajov ("Personal Data Protection Office", hereinafter referred to only as "DPA").

Address: Hraničná 12, 820 07, Bratislava 27, email: statny.dozor@pdp.gov.sk, www.dataprotection.gov.sk

The DPA is an independent central administrative body empowered to oversee compliance with the Act. The DPA is entitled to perform investigations in order to evaluate such compliance (including on-site investigations), to issue decisions on administrative offences under the Privacy Act, and to impose fines and other measures for its violations. DPA receives complaints regarding alleged violations of the Privacy Act and conducts proceedings regarding alleged violations of individuals' subjective rights in connection with the Privacy Act. The DPA also maintains register of personal data processing operations. Furthermore, the DPA issues recommendations for data controllers, provides methodical instructions for data controllers and data processors and provides consultations in the area of personal data protection.

Generally, the DPA will only have authority over cloud customers and cloud providers located in the territory of Slovakia. The DPA will also have authority over data processing that occurs on the territory of Slovakia even if the data controller – cloud customer is established outside the territory of the EU (e.g. in the USA) but carries out processing on the territory of Slovakia through a local (Slovakia-based) data processor – cloud provider (unless where it is merely a transit through the territory of the European Union).

3

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

The criteria correspond to those contained in the EU Data Protection Directive as described in response to question 2 in the EU Data Privacy Law section.

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 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: identification data of the parties; the date as of which the data processor is authorized to perform the processing; the purpose of the processing; name of the information system; the list of personal data to be processed/scope of processing; scope of data subjects; terms and conditions of the processing including a list of authorized operations; declaration of the data controller that the data controller considered professional, technical, organizational and personal capability of the data processor while selecting the data processor; data controller's consent with sub-processing (if applicable); the term of the processing; and date of signature of the agreement.

If the data controller authorized the data processor to process personal data after their collection, it must notify data subjects thereof at its first contact with the data subjects or within three months' period, at the latest. This applies also in case that data processing is taken over by the data controller's legal successor. The notification may be provided to data subject by the data processor.

5

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

While the Privacy Act is largely technologically neutral, elementary standards and measures are nevertheless listed. All security measures should be documented. Any employees or other persons coming into contact with personal data ("authorized persons") must be duly and manifestly instructed about the rights and obligations arising from the Privacy Act, scope of their authorization, list of permitted operations, conditions of processing and their liability for any violations thereof.

If the data controller processes sensitive data or if the information system is used for the purposes in public interest (e.g. public defense, public order), the data controller must document the security measures in the so called *security project*. The security project defines the scope and manner of the safety measures necessary for elimination and minimization of threats and risks affecting the filing system in terms of security breaches, reliability and functionality. The DPA has issued a Decree no. 164/2013 on scope and documentation of security measures of 13 June 2013 (the Decree 164/2013)[1] which is binding on all data controllers and which includes specific requirements for security project. Specific technical and organization measures include particularly the following:

- Cryptographic protection of the content of personal data carriers and cryptographic protection of data transferred via computer networks;
- Recording of access to the filing system by authorized individuals;
- Detection of malicious code presence in an incoming electronic post and in other files which are received from publicly accessible computer network or from other data carriers and protection against spam;
- Protection of external and internal environment by means of network security tool (e.g. firewall);
- Functionality of the backup data carrier check creation of backups with a predetermined frequency and recovery of the filing system backup check;
- Specification of personal data destruction processes with specification related to liability of particular entitled persons (safe deleting of personal data from the data carriers, destruction of data carriers and physical carriers of personal data);
- Procedure for reporting of security incidents and determined vulnerabilities of the filing system for the purposes of early adoption of preventive or remedial measures and keeping records thereof;

1 The full text of the decree in English will be soon available at: http://www.dataprotection.gov.sk.

- Inspection activity of the processor aimed at following of the adopted safety measures with specialization of the manner, form and periodicity of its realization (e.g. regular inspections of access to the filing system).

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?

No. Apart from the general obligation to notify to the DPA any intended automated data processing operations, including any proposed transfers of data to third countries, prior to the very commencement of the data processing, no other specific ad hoc approval or notification to the DPA of a data transfer outside the EEA based on EU Standard Contractual Clauses or the EU-US Safe Harbor Framework is required.

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.

In addition, the Privacy Act provides for a specific transfer regime for sensitive data: a data controller may transfer sensitive personal data to a third party established in a third country only with a prior written consent of the data subject unless otherwise stipulated by specific laws.

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?

In what concerns transfer of sensitive personal data to third countries, please refer to the response to question 7 above. Furthermore, the Privacy Act regulates certain types of sensitive data in more detail.

Birth number and similar identificators may only be used if it is necessary for the purposes of processing and it is prohibited to publish

such identificators. Personal data relating to psychological identity of an individual may only be processed by a psychologist or other person authorized thereto by special laws. Similarly, personal data relating to criminal or administrative liability of a person may only be processed by persons authorized thereto by law.

Special rules apply to biometric data. Methodical decree of the DPA 6/2013 on processing of biometric data of 28 November 2013 states that information systems for processing of biometric data should not be connected to cloud computing solutions.

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.

Pursuant to the Slovak Act on Banks, Act no. 483/2011, as amended, information that is subject to bank secrecy may only be provided to third parties with a written consent of the bank's client (data subject).

Furthermore, the National Bank of Slovakia ("NBS") has issued the Methodological Instruction of the Banking Supervision Division No. 6/2004 on the utilization of outsourcing by banks ("NBS Methodological Instruction 6/2004")[2], which is very likely to apply to majority of cloud computing services. The key requirement is that detailed and regularly updated risk assessment and management plans must be in place. The NBS Methodological Instruction 6/2004 also sets out elementary requirements for an outsourcing contract, including especially the following specific requirements:

(i) Detailed description of the outsourced activities;

(ii) Liability/responsibility in the event of deficiencies and applicable sanctions;

2 The full text of the instruction in English is available at: http://www.nbs.sk/en/financial-market-supervision/banking-sector-supervision/recommendations-and-methodical-instructions/methodical-guidance/mi-of-the-banking-supervision-division-no-6-2004.

(iii) Safeguards for protection of the bank's clients' personal data and data covered by banking secrecy and regime of their treatment (including a model situation where the service provider would be providing outsourced services to multiple institutions, of which at least one is a bank);

(iv) The consent of a service provider with the control and audit of the services performance during the contract term (by the bank's internal control and internal audit unit as well as an external auditor);

(v) The possibility for banking supervisors (NBS) to control the service provider, including its sub-contractors, in particular with respect to the access to data.

In the event of possible termination of the contractual relationship of a service provider with a bank or any unforeseeable events, the bank should have prepared a contingency plan in order to ensure continued performance of the outsourced activities until the bank finds another service provider.

10

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

Yes. Pursuant to the NBS Methodological Instruction 6/2004, a bank should submit to the Banking Supervision written information on its intention to outsource any of the activities supportive to the conduct of banking activities by another person.

A bank should inform the Banking Supervision in writing in particular of:

(i) Outsourcing of activities important for the bank, where a failure may have a clear impact on the bank's activities;

(ii) A failure of those outsourced activities which have a clear impact on the bank;

(iii) Serious problems with a service provider.

The notifications are not subject to any fees.

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. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies. The Privacy Act expressly prohibits combining personal data collected separately for different purposes.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply. The Privacy Act explicitly prohibits collecting personal data with the intention of their use for other purposes or activities than those explicitly declared upon their collection.

GUIDANCE NOTES AND RECOMMENDATIONS

13

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

No, the DPA has not issued any guidance on cloud computing.

PENDING LEGISLATION

14

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

No. However, as the amendment to the Privacy Act which took effect on April 15, 2014, has been contested, further amendments to the Privacy Act in the near future cannot be entirely excluded.

SLOVENIA

COUNSEL DETAILS:

Country: Republic of Slovenia
Attorney: Nastja Rovšek Srše
Law Firm: LAW FIRM KANALEC LTD.
Štefanova 5/V
1000 Ljubljana
Slovenia

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?

"Zakon o varstvu osebnih podatkov" (Personal Data Protection Act, Official Gazette of RS, No. 94/2007-UPB1, hereinafter referred to as the "Privacy Act"); unofficial English translation available here: https://www.ip-rs.si/index.php?id=339

The Slovene Privacy Act is substantially identical to the EU Directive.

2

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

"Informacijski pooblaščenec" (Information Commissioner of the Republic of Slovenia; hereinafter referred to as the "DPA")

Address: Zaloška 59, 1000 Ljubljana, Slovenia, gp.ip@ip-rs.si

The DPA is empowered to supervise the implementation of provisions of the Privacy Act (handling applications, notifications, giving explanations, etc.) and to react upon violations in this field. The DPA is also empowered to regulate the transfer of personal data to third countries (mainly managing administrative procedures for granting approvals, managing a list of third countries). Additionally, the DPA also manages and maintains a register of personal databases.

The DPA has authority over the cloud customers and cloud providers that are domiciled in the Republic of Slovenia. The DPA is also empowered to control the processing of personal data if the data controller (cloud customer) uses automated or other equipment located in the Republic of Slovenia, except where such equipment is used solely for the transfer of personal data across the territory of the Republic of Slovenia. Such data controller (cloud customer) must appoint a natural person or a legal person that has its seat or is registered in the Republic of Slovenia to represent it in respect of the processing of personal data.

3

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

The requirements for the applicability of the Privacy Act correspond to the principles described in the EU Data Privacy Law Section under question 2. Please see also our reply under question 2 above.

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 Privacy Act contains a specific requirement for the so called "traceability of processing of personal data" which represents one of the security measures determined in Privacy Act (please see also response to question 5 below).

Further, the Privacy Act requires that the data controller and data

processor enable subsequent determination when individual personal data were entered into a filing system, used or otherwise processed, and by whom; please see also response to question 5 below.

5

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

The Privacy Act requires the adoption of the following measures (the list is non-exhaustive):

(i) the protection of premises, equipment and systems software, including input-output units;

(ii) the protection of software applications used to process personal data;

(iii) the prevention of unauthorized access to personal data during transmission thereof, including transmission via telecommunications means and networks;

(iv) effective methods of blocking, destruction, deletion or anonymization of personal data;

(v) the subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and by whom; such determination shall be made possible for the period corresponding to the statute of limitation applicable in the given case.

In cases of the processing of personal data accessible over telecommunications means or networks, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorizations of the data recipient.

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. Even if the data transfer is based on EU Standard Contractual Clauses (or Binding Corporate Rules), it is mandatory to obtain the DPA's permission for such transfer outside the EEA. Obtaining of such specific transfer permission from the DPA takes approximately two months and the application is subject to an administrative fee of EUR 22.66.

No specific DPA approval or notification is required for transfers under the EU-US Safe Harbor Framework; however, the DPA in its guideline advises precaution and additional verification of whether the Privacy Act's provisions on security measures are complied with.

Further, approval is not required if personal data are transferred to countries which are listed on the so called adequacy list that is available at: https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/seznam-tretjih-drzav-66-clen-zvop-1/

Currently, the following countries are on the above-mentioned adequacy list: Switzerland, Republic of Croatia (still on the list even if now in the EU), the USA within the frames of the EU-US Safe Harbor Framework, and the Republic of Macedonia.

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.

Please refer to the response to question 6 above. There are no further specific requirements.

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 imposes additional measures for the processing of sensitive data: sensitive personal data must be explicitly marked and protected during processing in order to prevent access to such data by unauthorized persons, unless the individual to whom such data pertain published them himself/herself.

Sensitive personal data transmitted over telecommunications networks are considered adequately protected if they are sent with the use of cryptographic methods and electronic signatures which render such data illegible or anonymous during transmission.

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.

Outsourcing (which would include cloud computing) by banks is regulated by the Council of the Bank of Slovenia's *Decision on the risk management and implementation of the process of evaluation of appropriate internal capital for banks and savings banks (Official Gazette of RS, No. 104/2007 and subsequent amendments*; hereinafter referred to as the "Decision") that has been adopted pursuant to the Banking Act (Official Gazette of RS, No. 131/2006 and subsequent amendments). The Decision requires that the banks:

(i) adopt a relevant policy with the prescribed contents and a documented plan of use of outsourcing;

(ii) organize the use of outsourcers in a manner that allows for the constant monitoring of their activities and their risk management;

(iii) contractually reserve the rights to terminate the outsourcing relationship early at the bank's request;

(iv) contractually oblige the outsourcer to protect the bank's data, to ensure compliance with applicable legislation and regulations, to guarantee the bank's full access to the premises and data of the outsourcer as well as its unlimited right to inspect the premises and audit data;

(v) conclude a Service Level Agreement with the provider;

(vi) notify, the intended use of cloud computing to the Bank of Slovenia for verification of compliance (see response to next question).

The Insurance Act (Official Gazette of RS, No. 13/2000 and subsequent amendments) requires insurance companies to conclude a contract on outsourcing in case of the transfer of part of their business to an outsourcer. Such outsourcing requires the approval of the Insurance Supervisory Agency.

Pursuant to the Investment Funds and Management Companies Act (Official Gazette of RS, nos. 77/2011, 10/2012, 55/2012 and 96/2012) and the Financial Instruments Market Act (Official Gazette of RS, No. 108/2010 and subsequent amendments), the Securities Market Agency adopted relevant implementing regulations – *Decision on the transfer of performance of services or business* (Official Gazette of RS, No. 33/2012), which determines the conditions for the transfer of activities of investment funds and management companies, and the *Decision on the risk management and implementation of the process of evaluation of appropriate internal capital for brokerage companies* (Official Gazette of RS, No. 106/2007 and subsequent amendments), which applies to brokerage companies. Both decisions determine the conditions and requirements for outsourcing activities (use of cloud computing) in a similar manner as prescribed for banks, including a notification obligation (please see next question).

10

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

Yes. As outlined in response to question 9 above, the intended use of cloud computing by banks must be notified to the Bank of Slovenia to allow for verification of compliance. Similarly, investment funds, management and brokerage companies must notify intended deployment

of cloud computing to the Securities Market Agency.

Use of outsourcing (cloud computing) by insurance companies requires prior approval of the Insurance Supervisory Agency to allow for verification of compliance.

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. According to the Privacy Act, a cloud provider may perform individual tasks associated with the processing of personal data only within the scope of the cloud customer's authorizations, and may not process personal data for any other purpose. The principle of purpose specification and limitation, as described in response to question 10 of the EU Data Privacy Law section, applies.

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 same principles as outlined in response to question 11 of the EU Data Privacy Law section will apply.

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 Guidelines in Slovene can be found at:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf

The DPA Guidelines in English can be found at:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf

A summary of the guidelines for small companies (only in Slovene) can be found at:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Racunalnistvo_v_oblaku_-_povzetek_za_mala_podjetja.pdf

PENDING LEGISLATION

14

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

No.