CLOUD COMPUTING IN EASTERN EUROPE

2nd Edition

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 26 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:

- **Albania**, Eni Kalo, Kalo & Associates
- **Azerbaijan**, Ismail Zargarli, Fuad Aliyev, OMNI Law Firm
- **Belarus**, Alexey Anischenko, Sorainen
- **Bosnia & Herzegovina**, Anisa Tomic, Marić & Co
- **Bulgaria**, Nikolay Zisov, Boyanov & Co., Attorneys at Law
- **Croatia**, Olena Manuilenko, Ivan Ćuk, Vukmir & Associates, Attorneys-at-Law
- **Cyprus**, Anastasia Papadopoulou, Tassos Papadopoulos & Associates LLC
- **Estonia**, Hannes Vallikivi, Tark Grunte Sutkiene
- **Georgia**, Mikheil Gogeshvili, Mgaloblishvili Kipiani Dzidziguri
- **Greece**, Takis Kakouris, Zepos & Yannopoulos
- **Hungary**, Dóra Petrányi, Márton Domokos, CMS Cameron McKenna LLP
- **Kazakhstan**, Zhibek Aidymbekova, Norton Rose Fulbright
- **Latvia**, Vineta Čukste, Kronbergs & Čukste Attorneys at Law
- **Lithuania**, Iraida Žogaitė, Paulius Zapolskis, Baltic Legal Solutions Lithuania
- **Macedonia**, Prof. Valentin Pepeljugoski, Law Office Pepeljugoski
- **Malta**, Dr. Antoine Camilleri, Dr. Claude Micallef-Grimaud, Mamo TCV Advocates
- **Moldova**, Roger Gladei, Gladei & Partners
- **Montenegro**, Dragan Corac, Vujacic Law Offices
- **Poland**, Agata Szeliga, Sołtysiński Kawecki & Szlęzak
- **Romania**, Andreea Lisievici, Țuca Zbârcea & Asociații
- **Russia**, Georgy Moshiasvili, PIERSTONE

- **Serbia**, Marjan Poljak, Karanovic & Nikolic
- **Slovenia**, Nastja Rovšek Srše, Law Firm Kanalec Ltd.
- **Ukraine**, Iryna Kalyta, Ernst & Young

The article Cloud Computing – Brief Technical Overview for Legal Professionals was written by Zdeněk Jiříček, National Technology Officer at Microsoft s.r.o., 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 five 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 next 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. The last part of the publication consists of country-specific surveys of cloud-related data protection requirements in a number of selected non-EU countries.

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).
Convention	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, ETS 108, 1981 (http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm)
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 (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 26 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

Zdeněk Jiříček, National Technology Officer at Microsoft s.r.o., Czech Republic

INTRODUCTION

Cloud computing represents a huge paradigm shift in the way that computing power is provided to organizations and to end users. Rather than procuring their own hardware and software licenses, organizations now can choose 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 (hence balancing their power demand), 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:

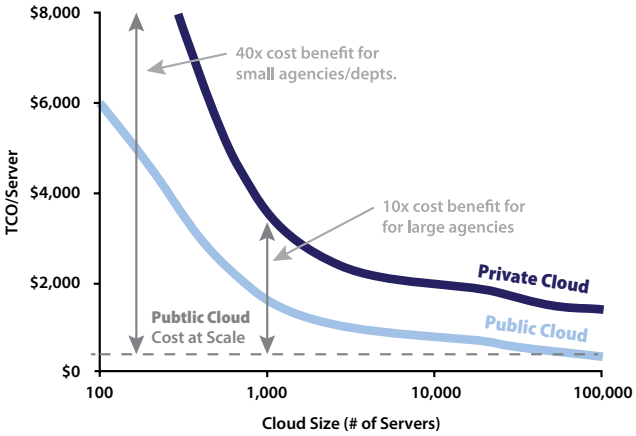


Figure 1: Cost per managed server – Small enterprise, Private, Public clouds[2]

2 Microsoft Corp.: The Economics of the Cloud For the EU Public Sector (2010), page 17http://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 99.98% in the year 2014 (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.

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:

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*

INTRODUCTION: CLOUD COMPUTING THROUGH THE PRISM OF EUROPEAN LAW

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.

This technological phenomenon has so far attracted only limited response from national legislators although local regulators start to take notice. In Europe, the European Union and the European Commission in particular, is a strong advocate of "unleashing the potential of cloud computing" by adopting strategies that aim to turn cloud computing into an engine for sustainable economic growth, innovation and cost-efficient public and private services. From EU 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. Most experts agree that, despite all its faults, the EU data protection law is one of the most stringent personal data privacy regime globally – if not the most stringent. As such it is not only relevant for countries which hope to join the EU in the future, but offers a high standard to aspire to, or a benchmark to measure

1 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.
2 Draft proposal for a regulation of the European Parliament and of the Council on the protection of individuals 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.

against: a company able to deal effectively with the requirements of the EU Data Protection Directive[1], and, in the years to come, the EU Data Protection Regulation[2], will likely be able to satisfy data privacy laws in other jurisdictions as well. In this sense, the draft EU Data Protection Regulation in particular aspires to set a new, truly global, privacy and data protection standard – a standard that is hoped to bring economic and social benefits to both consumers and companies operating in the digital world.

While the focus seems to be on the draft EU Data Protection Regulation, some believe that the new global privacy standard can be built upon another European legal instrument – the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. This Convention, opened for signature in 1981, obliges its signatories to enact legislation concerning the automatic processing of personal data. Given the number of signatories (more than 40 countries in Europe, including the Russian Federation, have ratified the Convention and it has influenced legislation far beyond Europe), it is sometimes believed to have a significant potential in shaping a truly international privacy standard. Not only have the Convention's fundamental standards stood the test of time; it's mechanism, notably the participation of various stakeholders, including states that are not parties to the Convention as well as non-state parties (such as the International Chamber of Commerce, the International Conference of Data Protection and Privacy Commissioners or the francophone association of data protection authorities), provides a unique framework for multilateral cooperation. The Consultative Committee, the T-PD, reflects on current issues brought about by the developing technologies by soft law instruments such as opinions, reports and recommendations. The Convention is currently under review; Ministers of Justice from 47 Council of Europe member states at their conference in Istanbul in November 2010 called for its modernization and strengthening as well as promoting its implementation worldwide. Among the key objectives of the modernization is to deal with challenges for privacy resulting from new technologies, and to strengthen the Convention's follow-up, enforcement mechanism. Countries from all over the world, NGOs, public and private sector have since been actively participating in the Convention's modernization process. Judging from the comments and proposals presented by the various stakeholders, cloud computing in particular is high on the agenda.

This article offers a view on selected legal aspects of cloud computing, primarily 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 software as a service (SaaS), platform as a service (PaaS) or infrastructure as a service (IaaS) 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. Where a cloud provider processes the entrusted personal data for its own purposes, for example for placing targeted advertisements, 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. 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, can be found in the national legislation of not only many EU Member States, but also some European countries that modelled their privacy laws on the EU Data Protection Directive.

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. Under the EU Data Protection Directive, 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 Council of Europe Convention. 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 former European Commissioner for Justice, Fundamental Rights and Citizenship. As calls for its suspension abound, 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[3]. 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 data exporters in the EU 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.

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

- **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 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.

ISO 27018: FIRST PRIVACY-SPECIFIC INTERNATIONAL STANDARD FOR CLOUD

In view of the above-mentioned cloud principles 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. 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, have been deployed by a number of global cloud providers. Until recently, however, there has been no comprehensive standard designed specifically for the processing of personal data in the cloud. This has changed with the new ISO/IEC 27018 set of rules adopted in August 2014 – the first ever standard for handling personal data in the cloud which has the potential to become a new global point of reference for assessing compliance of cloud services with data protection requirements.

ISO 27018 is applicable to the processing of personal data obtained from a customer for the purposes determined by the customer under its contract with the cloud service provider. It has been designed for all types and sizes of organizations and companies in private and public sector providing information processing services via cloud as personal data processors. It builds upon the ISO 27002 but sets out additional controls and associated guidance. These controls are listed under several categories,

including information security policies; human resource security; access control; cryptography; physical and environmental security; operations security (including areas such as protection from malware, back-ups, logging, monitoring and technical vulnerability management); communications security; and information security incident management. In addition, Annex A of ISO 27018 lists 11 principles that underpin privacy in cloud and that cover inter alia: the means of obtaining consent for processing personal data; purpose legitimacy and specification; data minimization; openness, transparency, and notice; data use and retention; or accountability.

This new privacy standard for cloud has been endorsed by some EU data protection authorities which see it as an important milestone in the field of security and protection of personal data in the cloud and believe that adherence to the standard will raise the confidence in cloud services.[4]

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;[5] 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

4 For example, the Statement of the Slovenian Data Protection Commissioner from January 9, 2015, available in Slovenian at https://www.ip-rs.si/priporocamo/detajl/iso-standard-za-ponudnike-racunalnistva-v-oblaku/?cHash=01331037243f496acb8e03a2143c9161
5 See, for example, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ or http://www.google.com/transparencyreport/removals/government/

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 aforementioned ISO 27018 standard aspires to set the new industry standard. While ISO 27018 does not account for any sector-specific requirements, and organizations in specialized industries such as public defense, financial or health services will probably have to apply additional sector-specific sets of controls, sectoral cloud providers are encouraged to develop their own protection controls based on the guiding principles contained in ISO 27018, taking their sector's specifics into account.[6] 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.

6 International Organization for Standardization recommends development of such independent controls, including direct cross-references to the relevant parts of ISO 27018. See for example https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en

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]

1 See definition of personal data in Article 2 (a) of EU Directive 95/46/EC.

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).

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.

A cloud provider is generally considered a data processor who processes 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: EU MEMBER STATES

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, Ivan Ćuk
Law Firm: Vukmir & Associates, Attorney-at-Law
Gramača 2L
10000 Zagreb
Croatia
Website: www.vukmir.net
E-mail: vukmir@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 on the Procedure for

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

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 163/2014 of the Czech National Bank on the performance of the activity of banks, credit unions and investment firms ("CNB Decree 163/2014")[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 163/2014 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 163/2014 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 163/2014, a prior notification to CNB is required if a financial institution subject to its supervision plans to deploy 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 published on the DPA's website on August 27, 2013 (available in Czech only at http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002;

DPA's Opinion on whether cloud computing may be used for processing of personal data from April 2, 2013, updated on July 23, 2014 (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?

While there is no pending legislation, a new Cyber Security Act entered into force on January 1, 2015. The new 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 new 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 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.

Similarly, the Strategic Framework of the Development of the Public Administration in the Czech Republic for 2014–2020[3] sets, as one of its specific goals, the completion of a functioning e-Government framework underpinned by cyber security standards and the 'open data' principle. It anticipates the implementation of the EU eIDAS (Electronic Identification and Signature), as well as amendments to the current legislation regulating e-Government.

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.
3 Document "*Strategický rámec rozvoje veřejné správy České Republiky pro období 2014-2020"* adopted by the Ministry of Interior in August 2014 and updated in January 2015

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/529012015008/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 Credit Institutions Act, client data not enabling the ascertaining of the data of a single client (e.g. encrypted data) is no longer considered a banking secret and can thus be stored on cloud servers as long as the service provider lacks access to the data and the general requirements of the Privacy Act are complied with. Banking secrets may also be disclosed by a credit institution to a third party 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?

No, there are currently no pending regulations concerning cloud computing. Further, the coalition agreement signed in April, 2015 includes no provisions for private sector cloud computing or data protection issues.

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 establishes the joint and several liability of the data processor (cloud provider) and data controller (cloud customer) as regards safety and security measures of the data processing, since the data controller is under the obligation to execute a data processing agreement with the data processor pursuant to which the latter contractually undertakes to comply with the data protection provisions aiming at the safety and security of the data.

The data processing operation between the data controller and data processor (if located outside the EU) requires a simple notification to the DPA if the processor is Safe Harbour 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?

An amendment to the Privacy Act is in progress but it is in a preliminary phase. A first draft was published by Ministry of Justice which is available for certain stakeholders to comment; however, the draft was not discussed by the Government or the Parliament at this stage.

The most important provisions of the proposed amendment are the following:

1. Binding Corporate Rules will be recognized as providing adequate protection in case of data transfers outside the EEA.

2. Data controllers – with the help of their internal data privacy officer, if appointed – shall keep internal records to verify the measures undertaken in connection with security breaches and to provide information to the people affected, if necessary. Such records shall include the relevant personal data, the number and range of the people affected, the date of the security breach, its circumstances and the measures taken to remedy the breach and other information set out in the regulations which required the data processing (if any).

3. The upper limit of the fine which can be imposed by the DPA should be HUF 20,000,000 (approx. EUR 74,074) – compared to the previous limit which was HUF 10,000,000 (approx. €37,037).

4. The proposed amendment provides more details on the case when the DPA may publish its decision (together with the data identifying the data controller). The DPA may be entitled to do so in case the decision affects a wide range of people, it pertains to the activities of public-sector entities or if such disclosure is justified by the gravity of the infringement.

5. According to the proposed amendment, the DPA will also be entitled - besides requesting information – to request a copy of the documents related to its investigation from the entities investigated.

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" ("Regulations 634" or the "Privacy Act").

Regulations of Cabinet of Ministers No. 40 of 30 January 2001 "Compulsory Technical and Organizational Measures of Personal Data Protection" ("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: Tark Grunte Sutkiene
Didžioji st. 23
LT-01128 Vilnius
Lithuania
Website: www.tarkgruntesutkiene.com
E-mail: Iraida.Zogaite@tgslegal.com, Paulius.Zapolskis@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?

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").

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, such approval is required. Transfer of personal data to data recipients in the third countries shall be subject to an authorization from the DPA, except for the cases provided in the Privacy Act; such authorization would be required even if the transfer is based on the EU Standard Contractual Clauses, BCR or the EU-US Safe Harbor Framework. The DPA shall grant or refuse to grant an authorization for transfer of personal data to third countries no later than within two months from the date of receipt of an application for the authorization by the data controller. An authorization shall be granted provided that there is an adequate level of legal protection of personal data in the third countries (for example, if the data controller relies on the EU-US Safe Harbor Framework, EU Standard Contractual Clauses, or Binding Corporate Rules).

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 was considering to adopt a cloud computing concept or guidelines but so far it is not clear if and when such concept or guidelines would be adopted..

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. Jasna 26
00-054 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 (in which case it must appoint a local data processor), 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 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?

As of January 1, 2015 there is no longer a need for DPA approval for the transfers outside of the EEA based on EU Standard Contractual Clauses. The DPA approval is still required for the transfers based on BCRs.

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 the DPA will follow the views presented in the European Union Court of Justice

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, the fact that there is no access to the content of data by the cloud provider due to the encryption, the fact that the service is not crucial from the perspective of the regulated entity's business continuity) 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. There is 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 allow the outsourcing of processing of medical documentation to third parties based on the same rules applicable to the outsourcing of personal data processing regulated by the Privacy Act, i.e. based on a data processing agreement which determines the scope and purpose of processing, appropriate technical and organizational measures, etc.

The Government is also working on the law which will specify the rules of video-monitoring in public areas and on implementation of intelligent metering systems in energy sector.

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: andreea.lisievici@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?

No. The requirements applicable to data processing and the data processing agreement under the Privacy Act are substantially similar to those under the EU Privacy Directive. Although the data processing agreement between the data controller and data processor does not require notification to the DPA, the processing of personal data itself must be notified (and, if applicable, authorised) by the DPA.[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 code, barcode, smart card). Authentication is mandatory for

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 The situations when the notification is not required are regulated through decisions issued by the DPA: Decision no. 23/2012, Decision nr. 100/2007. Decision no. 90/2006.
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.

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 health 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 health 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. However, an area of concern with potential important impact on cloud computing is the intention of the Romanian Intelligence Service to enact a law concerning cybersecurity. There has been an attempt to this end in December 2014, and the respective draft law included provisions requiring holders of "relevant data" (therefore including cloud services providers) to disclose such data to certain authorities and institutions, without any prior review or authorization by a court of law. This was one of the several reasons why the Romanian Constitutional Court found such law to infringe, among others, the constitutional right to private life. The draft law in question was found to be unconstitutional and did not enter into force, however representatives of the Romanian Intelligence Service have stated in March 2015 that work is under way for a new legislative proposal concerning cybersecurity.

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 is (is available) 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 amended the following year (effective as of 15 April 2014). Some of the changes introduced by the amendment 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 the security project. Specific technical and organization measures include particularly the following:

(i) Cryptographic protection of the content of personal data carriers and cryptographic protection of data transferred via computer networks;

(ii) Recording of access to the filing system by authorized individuals;

(iii) 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;

(iv) Protection of external and internal environment by means of network security tool (e.g. firewall);

(v) Functionality of the backup data carrier check creation of backups with a predetermined frequency and recovery of the filing system backup check;

(vi) 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);

(vii) 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 This Decree, which has been subsequently amended by Decree no. 123/2014, is available in Slovak at http://www.dataprotection.gov.sk

(vii) 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, DREN, ROVŠEK SRŠE Ltd.
Štefanova 5/V
1000 Ljubljana
Slovenia
Website: www.kdrs.si
E-mail: rovsek.srse@kdrs.si

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 Republic of Slovenia No. 94/2007-UPB1 (*Zakon o varstvu osebnih podatkov*, 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

https://www.ip-rs.si/priporocamo/detajl/iso-standard-za-ponudnike-racunalnistva-v-oblaku/?cHash=01331037243f496acb8e03a2143c9161

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.

COUNTRY SPECIFIC REQUIREMENTS BASED ON LOCAL PRIVACY LAW: SELECTED NON-EU COUNTRIES

ALBANIA

COUNSEL DETAILS:

Country: Albania
Attorney: Eni Kalo
Law Firm: Kalo & Associates
Kavaja Avenue, 4th Floor
G-KAM Business Centre
Tirana
Albania
Website: www.kalo-attorneys.com
E-mail: e.kalo@kalo-attorneys.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Law No. 9887, dated 10 March 2008 "On personal data protection", as amended (the "Privacy Act") and relevant by-laws. This legal framework sets out the rules and requirements applicable to "data processing" in the Republic of Albania. It provides the criteria of processing of personal data (including sensitive data), determines the legal purposes of processing, the exportation of personal data abroad, the rights of the data subjects during the processing of their personal data, the obligations of controllers/processors during their data processing activity.

The Privacy Act is to a large extent modelled upon the EU Data Protection Directive.

An English version of the Privacy Act is available at the following link: http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/ALBANIA_DPLaw2008.pdf

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or "DPA")? Summarize its powers.

The Privacy Act provides that the Information Data Protection Commissioner (hereinafter referred to as the "**DPA**") is the independent authority which is charged with the surveillance and monitoring of the protection of personal data by respecting and guaranteeing human rights and fundamental freedoms.

Under the Privacy Act, the DPA has the following duties:

(I) registering the controllers subject to the Privacy Act in the public register of controller; granting authorization for special categories of data (i.e. sensitive data) or special actions (i.e. international transfer to third countries);

(II) monitoring the protection of personal data: the DPA is entitled to perform administrative investigations (either ex officio or based on the claims of data subjects) and access personal data, and is entitled to collect all information necessary to fulfill this task. In case of unlawful processing of personal data the DPA may order the blocking, deletion, destruction or suspension of the further processing and may impose fines to controllers in accordance with the Privacy Act;

(III) issuing opinions on legal acts and regulations dealing with personal data; issuing guidelines determining, inter alia, data retention requirements in specific sectors; issuing guidelines for security measures in particular sectors of activity; promoting and explaining the rights for the protection of data and periodically publishing activity reports; ensuring the right information and the exercise of the right of correction and updating the database;

(IV) ensuring the cooperation with the supervisory personal data authorities of foreign countries to protect the rights of individuals residing in these countries; representing the supervisory authority in the field of protection of personal data in national and international activities.

3

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

The Privacy Act applies to controllers located in the Republic of Albania, but also to controllers not established in the Republic of Albania, which conduct their data processing activity through the use of any means, located in the Republic of Albania (i.e. affiliate, subsidiary, representative office, branch but also any technical mean such as hosts, servers located in Albania).

IMPORTANT DEFINITIONS

4

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?

The Privacy Act defines personal data as any information relating to an identified or identifiable physical person; 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. Under the Privacy Act, controllers of personal data have the legal obligation to notify their data processing activities to the DPA before commencing such activities. The notification is made through the submission of an official notification form which can be completed (in Albanian language) and submitted to the DPA online. Such notification should comprise the name and address of the controller, the scope of the processing, the categories of data subjects and the categories of personal data, the receivers and categories of receivers of personal data, the international transfers the controller intends to operate, and finally a general description of the safety measures for protection of personal data.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

The Privacy Act provides for the special category of sensitive data. This category is defined as any information about a physical person, concerning the origin of his race or ethnic origin, political opinions, membership of trade unions, religious or philosophical belief, criminal conviction, as well as data on health and sex life. Sensitive data can be processed only if:

(i) the data subject has given consent, which may be revoked at any time and makes it illegal further processing of data;

(ii) it is in the vital interests of the data subject or of another person and the data subject is physically or mentally incapable of giving his consent;

(iii) it is authorized by the authority responsible for an important public interest;

(iv) it relates to data which are manifestly made public by the data subject or is necessary for the exercise or defense of legal rights;

(v) the data is processed for scientific or statistical purposes;

(vi) the data is required for the purposes of preventive medicine, medical diagnosis, health care insurance, treatment, management of health care services and their use by medical personnel or other persons who have a duty of confidentiality;

(vii) the data is processed by a non-profit political, philosophical, religious organization or trade union for the purposes of their legitimate activities, only for members, sponsors or other persons related to their activity. These data will not be disclosed to a third party without the consent of the data subject, unless otherwise provided by law;

(viii) the processing is necessary for the fulfillment of legal obligations and specific rights of the controller in the field of employment, in accordance with the Labor Code.

If none of the conditions above is fulfilled, the processing of such sensitive data requires authorization by the DPA.

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

6

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

As defined by the Privacy Act, "controller" means any natural or legal person, public authority, agency or other entity who, alone or with others, determines the scopes and the means of processing of personal data, in compliance with relevant laws and by-laws, and who is responsible for the performance of the obligations provided by the Privacy Act. On the other hand,4.5. "Processor" is defined as any natural or legal person, public authority, agency or any other entity that processes data on the behalf of the controller. Based on these definition cloud customers generally qualify as "controller" and cloud customer as "processor".

Under the Privacy Act, controllers may hire data processors to lawfully process personal data, in compliance with the instructions provided by controller.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes. The obligations of the processor shall be defined in a written processing agreement between the data controller and the data processor. The relation between the data controller and data processor is regulated by the provisions of the DPA's Instruction No. 19, dated 03.08.2012 "On relation between data in case of delegation of processing of personal data and the use of a template agreement in the ambit of such delegation", as amended (hereinafter referred to as the "Instruction No.19"). Instruction No. 19 also provides a template agreement that shall be signed by the controller and processor in the ambit of such delegation of data processing. Such agreement ensures that the processor uses and discloses personal data only under the

instructions of the controller and undertakes all measures to ensure the adequate protection of such data. The use of the template agreement, however, is not mandatory, and the data controller and processor may use their own agreement as long as all the prerequisites set forth in Instruction No. 19 are met.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Under Instruction No.19, the use of sub-processors by data processors is permissible, but only upon the prior approval of the controller. In this case the sub-processor shall be subject to the same obligations that are applicable to the processor, and the relation between the processor and sub-processor shall be formalized under a written agreement, which shall include the prior approval of the controller and also the prior verification of the controller that the sub-processor guarantees the same level of security of personal data as the processor (i.e. a lower level of security would not be accepted).

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

As a general principle, the Privacy Act allows a cross-border transfer of personal data only to such recipient countries which guarantee an adequate protection of personal data. A list of countries which guarantee an adequate protection of personal data is provided by Decision No.934, dated 2 September 2009 "On the determination of the countries which have a sufficient level of personal data protection" (hereinafter referred to as „Decision No.943"). According to this Decision, these "safe" countries are inter alia the members of the EU and the members of the European Economic Area (EEA). The transfer to any EU Member State can be made without having to obtain any prior authorization from the DPA. However, it is part of the data controller's general notification obligation (please refer to question 4 above) to indicate an intended transfer to the EU in the relevant section of the official notification form.

10

What are the requirements to transfer personal data to a non-EU country?

In addition to the EU countries, the countries which guarantee an adequate protection of personal data (listed in the Decision No.934, dated 2 September 2009 "On the determination of the countries which have a sufficient level of personal data protection") also include members of the European Economic Area (EEA), countries which have ratified the Convention, and countries to which personal data can be transferred according to a decision of the European Commission. It means that personal data can be transferred without the DPA's prior approval to recipients established in the USA that are Safe Harbor certified. The full list of these countries is available in this Decision and may be also requested from the DPA upon request.

Notwithstanding the general principle of international transfer set out above, the Privacy Act has taken into consideration the necessity of the controllers to transfer personal data to third countries (i.e. countries that do not guarantee a sufficient level of protection of personal data) and has provided the rules for such transfer accordingly. The controller transferring personal data to third countries must obtain prior authorization from the DPA. Otherwise, international transfer of personal data to a country that does not have sufficient protection level of data is permissible (without seeking any authorization from the DPA) if one of the conditions set out below is met:

(i) it is authorized under international acts, ratified by the Republic of Albania and immediately applicable;

(ii) the person to whom the personal data belongs has given his consent for the international transfer;

(iii) it constitutes an obligation for the execution of a contract concluded between the controller and the person to whom the personal data belongs or a third party, in the interest of the person to whom the personal data belongs;

(iv) it constitutes a legal obligation for the controller;

(v) it is necessary for the protection of the vital interest of the person to whom the personal data belongs;

(vi) it is necessary or constitutes a legal requirement for an important public interest or for the exercising and protection of a legal right;

(vii) it is made from a register which may be used for consulting and provides information the general public.

If none of the conditions above is met, then the transfer to a non-EU country requires authorization by the DPA.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

Under the Privacy Act the data controller and processor must take appropriate organizational and technical measures to protect personal data against unlawful, accidental destruction, accidental loss, any unauthorized access or disclosure, in particular when data processing is done on a network, as well as from any other form of unlawful processing. Such special security measures include:

(i) defining organizational units functions and operators for the use of data;

(ii) using data upon the order of organizational units or authorized operators;

(iii) instructing operators, without exception, about the obligations they have in accordance with the Privacy Act and relevant bylaws, including regulations for data security;

(iv) prohibiting entry by unauthorized persons onto the premises of the controllers/processors;

(v) permitting the access to data and programs only to authorized persons,

(vi) prohibiting the access into the archiving tools and their use by unauthorized persons;

(vii) operating data processing equipment upon authorization only and securing every device with preventive measures against unauthorized operation;

(viii) recording and documenting any modifications, corrections, deletions, transmissions of personal data.

every device shall be secured with preventive measures against unauthorized operation;

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

Yes. Instruction No.19 (please refer to question 7 above) provides that in the agreement between the controller and the processor, the latter shall undertake all security measures (please refer to question 11 above) that are necessary to guarantee the adequate protection of personal data.

OTHER REQUIREMENTS

13

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

No. Under the Privacy Act, data processors are obliged to process the data only in accordance with the instructions of the controller and may not transmit them, except when taking instruction from the controller. It means that the processor cannot use the data obtained from the controller for marketing purposes, unless the controller instructs the processor to do so (i.e. in this case the controller must first have obtained the data subjects' consent with the processing of personal data for marketing purposes).

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

Under the Privacy Act, the processor hired by the controller is obliged to make available to the controller all the necessary information as to allow the latter to check compliance with all relevant obligations under the Privacy Act. As it derives from this provision, the controller is entitled to monitor the activity of the processor to ensure the compliance with the applicable legal requirements. The controller and the processor are free to determine in the data processing agreement how this control will be exercised, i.e. nothing prevents the parties to agree to an audit by an independent auditor selected by the cloud provider.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

Under Instruction No. 19, prior to delegating the data processing to a processor, the controller must inform the DPA on such delegation in compliance with the Privacy Act.

PUBLIC SECTOR

16

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

No. According to the Instruction No.19, a controller is defined as the natural or legal person, public authority, agency, company, organization or institution that retains, manages and controls personal data and which for the scope of processing of such data enters into a contractual relation with a third company that in this case will be considered as the data processor. The above definition indicates that no distinction is made between public and private sector (i.e. requirements related to the delegation of personal data for the scope of processing, equally apply to private entities but also the public ones).

FINANCIAL DATA

17

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.

Instruction No.20, dated 03.08.2012 "On the processing of personal data in the banking sector" (hereinafter referred to as „Instruction No.20") provides specific rules for the processing of personal data by financial institutions. It does not, however, provide any specific requirement on the use of cloud computing by a financial institution (or, generally, any rules on outsourcing that may be applied to a cloud computing scenario). In the absence of requirements applicable to financial institutions sector specifically, the general requirements imposed by Instruction No.19 would apply to this category of controllers (see question 7 *et seq.*).

18

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

Apart from the general notification obligation applicable to all data controllers (please refer to question 15 above) there is no notification or approval required for the use of cloud computing specifically.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

No, currently there is no guidance specifically addressing cloud computing issued by the DPA. As the DPA tends to monitor closely any technology developments, it cannot be exclude that it will issue a cloud-related guidance in the near future.

PENDING LEGISLATION

20

Is there any pending legislation that will have significant impact on cloud computing?	No.

AZERBAIJAN

COUNSEL DETAILS:

Country: Azerbaijan

Attorney: Ismail Zargarli, Fuad Aliyev
OMNI Law Firm
Bridge Plaza, 8th Floor
6 Bakikhanov street
Baku, AZ 1065
Azerbaijan

Website: www.omnilawfirm.com

E-mail: izargarli@omnilawfirm.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

The Law of the Republic of Azerbaijan on Personal Data (*Fərdi məlumatlar haqqında Qanun*) dated 11 May 2010 (the "Privacy Act"). A number of legislative acts have been enacted in furtherance of the Privacy Act regulating certain aspects of the personal data protection such as Decrees of the President of the Republic of Azerbaijan on "Application of the law on personal data", "Enforcement of the law on personal data", and subsequent decrees on "Amending the decree on application of the law on personal data", "Approval of the rules on conducting the register of personal data information systems", "Resolutions of the Cabinet of Ministers of the Republic of Azerbaijan on approval of requirements of protection of personal data", or "Rules on state registration and annulment of personal data information systems".

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or "DPA")? Summarize its powers.

The supervisory competencies are not strictly defined in law. Ministry of Communications and High Technologies of the Republic of Azerbaijan (http://www.mincom.gov.az/home/) would be the main state authority overseeing the compliance with the Privacy Act. However, certain other state authorities may also have supervisory competencies in the field of the Privacy Act.

The Decree of the President of the Republic of Azerbaijan on Implementation of the Law of the Republic of Azerbaijan on Personal Data, No. 275 dated 4 June 2010 ("Decree No. 275") provides that:

(i) The President of the Republic of Azerbaijan has the authority to determine rules for maintaining the state register of personal data information systems;

(ii) The Cabinet of Ministers of the Republic of Azerbaijan has the authority, inter alia, to:

a. determine requirements for protection of personal data;

b. determine the rules for disclosure of personal data collected in and processed in corporate information systems to third parties based on payment;

c. determine the scope and rules for transfer of information on financial transactions of foreign legal entities and individuals in Azerbaijan pursuant to international agreements of the Republic of Azerbaijan;

d. determine the rules for the state registration of personal data information systems and rules for personal data information systems which shall not be registered with the state register of personal data information systems, rules for destruction of data in personal data information systems which have been de-registered from the state register of personal data information systems.

Further, the Decree of the President of the Republic of Azerbaijan on "Ensuring Implementation of the Law of the Republic of Azerbaijan on Personal Data, No. 361 dated 13 December 2010" ("Decree No. 361") provides that,

(i) the Ministry of Communications and High Technologies of the Republic of Azerbaijan has the authority to:

a. request the withdrawal of personal data from information systems of common use if such information was received through open sources;

b. receive complaints of individuals relating to the processing of their personal data;

a. conduct state registration and maintain state register of personal data information systems.

(ii) the Ministry of Communications and High Technologies, the Ministry of National Security, the Ministry of Internal Affairs, the Ministry of Justice and the State Special Protection Service of the Republic of Azerbaijan, acting within the scope of their responsibilities, have the authority, inter alia, to:

a. check compliance of the collection, processing and protection of personal data with the requirements of the Privacy Act and with the declared purposes of information systems;

b. make inquiries with the owners (controllers) and operators of personal data or obtain necessary data from state authorities, owners or operators of personal data free of charge;

(iii) enforce compliance of state authorities, legal entities and individuals engaged in the collection, processing and protection of personal data with the Privacy Act.

3

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

The Privacy Act applies to collection, processing and protection of personal data, including cross-border transfer by the state authorities, individuals and legal entities. It does not apply to:

(i) collection and processing of personal data by individuals exclusively for personal or family needs;

(ii) collection and processing of personal data in connection with national security, law enforcement, intelligence and counter-intelligence activities; and

(iii) protection of personal data related to state secrets and national archives.

The Privacy Act does not contain any provisions related to territorial applicability. It can nevertheless be concluded that the Privacy Act would apply to all owners (controllers) and operators of personal data that are citizens, legal entities and state and local government authorities established on the territory of Azerbaijan. For the definition of "owner" and "operator", see question 6.

IMPORTANT DEFINITIONS

4

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 is defined as any data that allows directly and indirectly identifying a person. The law offers no guidance on whether encrypted data falls within the definition of personal data if cloud provider does not have an encryption key.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

There are 2 categories of personal data: (i) open personal data and (ii) confidential personal data.

Open personal data includes: (i) data depersonalized in accordance with the law; (ii) data which is declared to be open by a person to which such personal data relates ("personal data subject") or (iii) data entered into the public information system upon consent of the personal data subject. Name, family name and patronymic of a person are considered open personal data. The law does not require confidentiality of open personal data.

While the Privacy Act does not stipulate so explicitly, it can be concluded from the wording of the Privacy Act that any other personal data is considered confidential personal data. Confidential personal data must be protected in accordance with the requirements of legislation by the owner, operator of personal data, and users having access to such data. Confidential personal data can be provided to third parties only with the consent of the personal data subject, except for cases stipulated by law.

Further, the legislation also provides that information about race, nationality, family life, religious faith and belief, health or imprisonment records of an individual are considered "personal data of special category". Personal data of special category are to be treated either as confidential or open depending on the type of the information and circumstances of disclosure.

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

6

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

The Privacy Act's term equivalent to a "data controller" is the "owner of the personal data". The "owner of personal data" is a state authority, local self-governance authority, legal entity or individual that (i) exercises the full right of possession, use and disposal of the personal data

information system or reserve and (ii) determines the purpose of processing of personal data.

The Privacy Act's term equivalent to a "data processor" is the "operator of personal data". The operator of personal data is defined as (i) the owner of personal data who collects, processes or protects the personal data; or (ii) the state authority, local self-governance authority, legal entity or individual who is authorized by the owner of personal data to conduct such activities within certain scope and under certain conditions.

Thus, in the context of cloud computing, the cloud customer would generally be considered the "owner of personal data" while the cloud provider would be mostly in the position of the "operator of personal data".

The key obligations of the owner of personal data are:

(i) to ensure safety and legality of collection and processing of personal data;

(ii) to protect (including against accidental or unauthorized destruction, loss, illegal interference, change etc.) confidential personal data at the level established by the legislation;

(iii) to obtain written consent of the personal data subject for collection, processing and transfer of personal data;

(iv) respond to queries of the Ministry of Communications and High Technologies of the Republic of Azerbaijan;

(v) to provide to the personal data subject information on:

a. existence and contents of personal data that the owner process and that relate to the personal data subject;

b. legal grounds for collection, processing and transfer of personal data to third parties;

c. purposes of collection and processing of personal data, terms and methods of processing;

d. persons authorized to view personal data and information systems which are included in the personal data exchange;

e. source of personal data;

f. proof of legality of personal data;

g. certificate of conformity and state expertise of information system;

h. information about the owner and the operator;

(vi) to correct, destruct, transfer to archive, stop collection and processing of personal data at the request of the personal data subject.

The key obligations of the operator of personal data are:

(i) to ensure safety and legality of collection and processing of personal data;

(ii) to protect (including against accidental or unauthorized destruction, loss, illegal interference, change etc.) confidential personal data at the level established by the legislation;

(iii) to obtain a written consent (where such is required by the Privacy Act) from the personal data subject for collection, processing and transfer of personal data;

(iv) to provide conditions for intelligence and counter-intelligence activities, law enforcement activities in the manner provided in the legislation of the Republic of Azerbaijan and to resolve related technical and organizational issues;

(v) to advise the personal data subject of the contents and source of the personal data if personal data in information system of common use is received from open sources;

(vi) to inform the personal data subject in the same scope as outlined above for data owners.

In many instances the law is not specific about whether the aforementioned obligations pertain only to the owner or the operator of personal data, or to both.

The owner or operator shall register personal data information systems (with certain exceptions) with the Ministry of Communications and High Technologies. Furthermore, any activity related to creation of databases containing personal data and of personal data information systems, as well as "servicing" such information systems is subject to obtaining license from the Ministry of Communications and High Technologies. The legislation is not clear whether the license shall be obtained by the owner or the operator or whether this requirement applies to foreign persons providing cloud computing services in Azerbaijan.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes. In the context of the owner – operator contractual relationship in cloud computing, the cloud customer would generally be considered the "owner of personal data" while the cloud provider would be mostly in the position of the "operator of personal data".

Under the Privacy Act, the owner can entrust the operator with the collection and processing of personal data on the basis of an agreement, provided that the protection of personal data is ensured through adequate safeguards. The obligations of the operator shall be stipulated in the agreement concluded between the owner and the operator; the Privacy Act does not prescribe any minimum content of such agreement.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

The Privacy Act does not explicitly regulate sub-processing. It can thus be deemed generally permissible provided all required data protection measures and other obligations under the Privacy Act and the implementing legislation are met.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

There are no differences in requirements for the transfer of personal data to EU or non-EU countries.

The Privacy Act prohibits cross-border transfer of personal data, if

(i) transfer of personal data causes threat to the national security of the Republic of Azerbaijan;

(ii) the laws of the country to which the personal data is transferred provide for lesser legal protection of the personal data than under Azerbaijani legislation.

However, under the Privacy Act, if the personal data subject agrees to a cross-border transfer of the personal data or the cross-border transfer of personal data is required for protection of life and health of the personal subject data, the personal data can be transferred regardless of the level of legal protection afforded by such foreign country.

10

What are the requirements to transfer personal data to a non-EU country?

Please see response to question 9 above.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

The Privacy Act merely stipulates that the owners and operators shall implement both technical and organizational measures for the protection of personal data. These security measures, applicable to collection, processing, distribution and transfer of personal data, are then set forth in the Resolution of the Cabinet of Ministers of the Republic of Azerbaijan on Approval of Requirements to Protection of Personal Data, No 161 dated 6 September 2010 (Resolution No. 161). These requirements include, *inter alia*:

Technical and organizational security measures during processing of personal data:

(i) Exclusion of interference that can disrupt work of automated technical facilities used for processing of personal data;

(ii) Timely detection of illegal interference with personal data, prevention of unauthorized copying or transfer;

(iii) Ensuring possibility to restore modified or destroyed personal data;

(iv) Processing of personal data only by software and in accordance with instructions tested and approved by the owner of personal data;

(v) Use of certified data security equipment/ facilities and methods;

(vi) Maintaining records of used data security equipment/ facilities, documentation, bearers of personal data;

(vii) Maintaining records of persons authorized to work with personal data, requiring such persons to undertake not to disclose personal data during work or after completion of contract;

(viii) Investigate breach of confidentiality of personal data and other instances that result in a decrease of the level of protection of

the personal data, taking measures to eliminate "threatening" consequences of such breach;

(ix) Provision of reserve power systems and fire-safety signaling at the premises where personal data is stored;

(x) Provision of access to users of personal data through "security" servers of owner/operator;

(xi) Use of 256 b encryptions keys for transfer of information;

(xii) State expertise of project documentation for personal data information systems.

The Resolution No. 161 further provides that state authorities shall conduct monitoring of correctness of security measures for protection of personal data information systems at least once a year. These authorities are the Ministry of Communications and High Technologies of the Republic of Azerbaijan, the Ministry of National Security of the Republic of Azerbaijan, the Ministry of Internal Affairs of the Republic of Azerbaijan, the Ministry of Justice of the Republic of Azerbaijan and the State Special Protection Service of the Republic of Azerbaijan.

Furthermore, the Privacy Act provides that an owner and/or operator shall ensure that all transactions related to collection, processing, inquiries and access to personal data, requests, management and security of information systems shall be recorded in the relevant control and audit logs.

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

There are no laws / regulations imposing specific security requirements on cloud providers. However, sectoral regulation applies to state secrets, security of information systems, banking secrets, information related to national security and law enforcement, or archiving of data that may be of relevance if such data were to be stored in the cloud.

OTHER REQUIREMENTS

13

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

While there is no explicit regulation around personal data mining, generally, personal data must always be collected in compliance with the law and for specified, explicit and legitimate purposes and not further processed in a way incompatible with the law. A data processor that has been entrusted by its customer solely with the processing of the customer data in the cloud is bound by the customer's instructions and may not mine customer data for its own advertising purposes.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

The customer has no legally established right to audit the cloud provider. An audit right would have to be stipulated in the agreement between the customer and the cloud provider.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

While there is no notification or approval required for the use of cloud services specifically, under the Privacy Act, all personal data information systems must be registered with the Ministry of Communications and High Technologies. The Ministry is entitled to check the information provided by the owner, the compliance of the information systems with the initial plan, and to conduct a state expertise of the information systems in accordance with the legislation.

PUBLIC SECTOR

16

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

There are no different requirements under the Privacy Act. Public sectors customer could be subject to laws governing national security, state secrets, law enforcement, archiving etc.

FINANCIAL DATA

17

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 Central Bank of Azerbaijan has enacted Rules on Use of Information Technologies at Banks (the "Rules"). The Rules provide that all banks shall build their IT systems and ensure their security in compliance with the Rules. The Rules sets forth provisions on main requirements in relation to information systems and information technologies, access to data in the information systems, procedures for emergency situations, risk management and information security.

The Privacy Act provides that information about financial transactions of foreign nationals in the Republic of Azerbaijan is to be provided to relevant foreign authorities as provided in the international treaties to which Republic of Azerbaijan is a party.

Further, the Law of the Republic of Azerbaijan on Banks provides that "documents allowing to identify a client, as well as documents allowing to confirm settlement and transfer transactions of the client shall be kept at the bank for at least five years after termination of mutual relationships with the client and completion of payments (transfers)". This retention requirement, if interpreted restrictively, could be viewed as a strict obligation to keep the said documentation within the bank's premises or systems, thus effectively barring the storage of such data in the cloud.

18

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

The Rules provide that a bank shall provide to the Central Bank of Azerbaijan (regulator) report on information technologies used by the bank. This would likely include information concerning the deployment of a cloud solution.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

There is no generally accessible guidance on cloud computing.

PENDING LEGISLATION

20

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

No. There is no pending legislation pertinent to cloud computing that is expected to be enacted in 2015.

BELARUS

COUNSEL DETAILS:

Country: Republic of Belarus
Attorney: Alexey Anischenko
Law Firm: Sorainen
Nemiga street, 40
220004 Minsk
Republic of Belarus
Website: www.sorainen.com
E-mail: alexey.anischenko@sorainen.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Law on Information, Informatisation and Information Protection (*Закон Республики Беларусь «Об информации, информатизации и защите информации»*) No. 455-Z of 10 November 2008.

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or "DPA")? Summarize its powers.

There are two authorities which primarily oversee the data protection law: The Operational and Analytical Center under the Aegis of the President (*Оперативно-аналитический центр при Президенте Республики Беларусь*) and the Ministry of Communications and Informatisation (*Министерство связи и информатизации Республики Беларусь*).

Address: Kirova street 49, 220030 Minsk; web: http://oac.gov.by/; email: obr@oac.gov.by

Address: Independence Avenue 10, 22050 Minsk; web: http://www.mpt.gov.by/en/; email: mpt@mpt.gov.by

The Operational and Analytical Center under the Aegis of the President has the following powers:

(i) to carry out state control in the sphere of inter-agency information interaction of state bodies;

(ii) to carry out state control and management in the sphere of technical and encrypted information protection;

(iii) to develop drafts of legal acts and adopt acts related to technical and encrypted information protection, etc.

(iv) The Ministry of Communications and Informatization has the powers to:

(v) set forth the requirements for compatibility of information resources, information systems and information networks:

(vi) organize the technical rate setting and standartization of information resources, information systems and information networks;

(vii) develop and adopt the guidelines of operation and interaction of information resources, information systems and information networks, etc.

3

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

The Privacy Act regulates social relations in the territory of Belarus involving both residents and non-residents arising from:

(i) finding, obtaining, transfer, collection, processing, accumulation, storage, distribution and (or) provision of information and use of information;

(ii) creation and use of information technologies, information systems and information networks, formation of information resources;

(iii) organization and provision of information protection.

Therefore, as long as the data processing occurs on the territory of Belarus, the Privacy Act would apply.

The Privacy Act covers not only the processing of personal data, but also information and information systems in general. Specific regulation provided in the Privacy Act then applies to personal data specifically (these are elaborated on in the responses to the following questions), data constituting state secrets, advertising, scientific and technical, statistical, legal and other information.

The Privacy Act does not apply to social relations connected to the activities of the media and protection of information which is subject to intellectual property rights.

IMPORTANT DEFINITIONS

4

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 basic and additional personal data of an individual that are required to be submitted to the Population Register in accordance with the law of Belarus, as well as other data allowing to identify an individual. Basic personal data include, for example, an individual's name, surname or date of birth; additional personal data include, for example, tax registration or education information.

Encrypted data would be regarded as personal data only if they fall within the above definition, irrespective of whether the cloud provider possesses access to the encryption key or not. If the data qualify as either basic or additional personal data, they will be automatically regarded as personal data even if they are encrypted and the cloud provider does not have the means to decrypt them.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

The Privacy Act does not differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data. There is no specific concept of sensitive personal data in Belarus.

At the same time specific requirements to personal data protection may be contained in secondary acts, e.g. regulation governing clinical trials.

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

6

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

The Privacy Act does not distinguish between data processors and data controllers for purposes of information protection.

The Privacy Act differentiates between the following subjects of information relations:

(i) information possessors;

(ii) users of information, information systems and/or information networks;

(iii) owners and possessors of program and technical tools, information resources, and information systems and networks;

(iv) information intermediaries;

(v) information systems operators.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes, The Privacy Act requires that the information possessor and the information user conclude an agreement. Such agreement typically includes terms and conditions of information use and liability for breach of such terms and conditions (as an information security measure). The requirement on agreement conclusion would apply to a cloud customer and cloud provider alike.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

The Privacy Act does not explicitly regulate sub-processing. It can thus be deemed permissible provided all required information protection measures are taken by the responsible parties.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

There are no specific requirements to transfer personal data to the EU. A general requirement that personal data can only be transferred with a written consent of an individual applies.

10

What are the requirements to transfer personal data to a non-EU country?

There are no specific requirements apart from the general requirement that personal data shall be transferred with a written consent of the individual concerned.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

Yes, it does. Organizational measures usually include a specific access regime to the premises where an access to the information can be gained as well as differentiation of information access based on level of access rights for employees and information characteristics.

Technical measures include usage of technical and encrypted information protection tools, as well as measures on information protection control. Encryption is mandatory in limited cases (e.g. storage and processing of state secrets). In other cases it is one of the measures that can be implemented as an alternative to other technical measures.

In addition, one of the legal measures to ensure security is the mandatory agreement between the information possessor (cloud customer) and the information user (cloud provider) as outlined in response to question 7 above.

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

No.

OTHER REQUIREMENTS

13

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

No, it is not. A cloud provider can mine customer data for advertising purposes only with the written consent of the individual whose personal data are mined.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

The customer has no legally established right to audit the cloud provider. An audit right would have to be stipulated in the agreement between the customer and the cloud provider.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

No, there are no prerequisites for a customer to use cloud services.

PUBLIC SECTOR

16

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

Public sector cloud customers are obliged to register information systems they use in accordance with the laws of Belarus (the registry is accessible at http://infores.mpt.gov.by/it/database_is/). Registration of private information systems is voluntary.

FINANCIAL DATA

17

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 key sector-specific legal requirement is an obligation to keep banking data secret which applies to financial institutions possessing financial data of their customers. There are no other publicly available legal regulations or guidelines that would prescribe specific requirements applicable to financial data that financial institutions need to be aware of

while using cloud computing. While the aforementioned secrecy regulation does not take into account outsourcing or cloud services specifically, it does not explicitly preclude financial institutions from outsourcing some of their functions and activities and it can be reasonably concluded that, subject to the cloud service provider maintaining the secrecy obligation, financial institutions may deploy a cloud solution.

18

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

No.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

Yes, there is a guidance for public sector (state bodies or organizations) embodied in the President Edict to execute a gradual transfer, until 31 December 2018, onto the state platform which resources are operated by Belarusian Cloud Computing LLC providing cloud computing services to the public sector (http://pravo.by/main.aspx?guid=12551&p0=P31400046&p1=1&p5=0). This requirement should not *per se* present a restriction to public sector organizations to deploy cloud services of a private cloud provider; however, there is no guidance on this issue.

PENDING LEGISLATION

20

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

No.

BOSNIA & HERZEGOVINA

COUNSEL DETAILS:

Country: Bosnia & Herzegovina
Attorney: Anisa Tomic
Law Firm: Marić & Co
Mehmeda Spahe 26
71000 Sarajevo
Bosnia & Herzegovina
Website: anisa.tomic@mariclaw.com
E-mail: www.mariclaw.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Law on Personal Data Protection of Bosnia and Herzegovina, published in the Official Gazette of Bosnia and Herzegovina no. 49/06 and 76/11 (the „Privacy Act") and related bylaws/rulebooks. The Privacy Act is based on the EU data privacy legislation, namely the EU Data Protection Directive.

An English version of the Privacy Act and related bylaws/rulebooks are available at:

http://www.azlp.gov.ba/propisi/Defaultaspx?id=5&pageIndex=1&langTag=en-US

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or the "DPA")? Summarize its powers.

Agencija za zaštitu ličnih podataka Bosne i Hercegovine (Personal Data Protection Agency of Bosnia and Herzegovina, hereinafter referred only as the „DPA").

Address: Vilsonovo šetalište broj 10, 71 000 Sarajevo
Website: http://www.azlp.gov.ba/Default.aspx?langTag=en_US&template_id=147&pageIndex=1, e-mail: azlpinfo@azlp.gov.ba

The DPA is entitled to:

(i) Perform supervision, through inspection, over fulfilment of obligations stipulated by the Privacy Act;

(ii) Keep the Central Registry of personal data controllers;

(iii) Accept incentives and complaints of citizens concerning breaches of the Privacy Act;

(iv) Adopt implementing regulations, guidelines or other legal documents in line with the Privacy Act;

(v) Order blocking, erasing or destroying of data, temporarily or permanently ban processing of data, issue warning or reprimand to the controller;

(vi) File a request for initiating misdemeanor proceedings pursuant to the Privacy Act;

(vii) Provide advice and opinions in the area of personal data protection;

(viii) Co-operate with similar authorities in other countries;

(ix) Exercise other duties as foreseen by law;

(x) Supervise the transfer of the personal data out of Bosnia and Herzegovina.

3

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

The Privacy Act explicitly stipulates the criteria for territorial applicability; namely, in accordance with its Article 1 the purpose of the Privacy Act is to secure, in the territory of Bosnia and Herzegovina, for every individual, regardless of his/her nationality or residence, respect for human rights and fundamental freedoms, and in particular the right to privacy with regard to the processing of personal data relating to him/her. Therefore it would apply to all entities that operate on the territory of Bosnia and Herzegovina. The applicability of Privacy Act is triggered by the place of establishment of the entity that is responsible for the processing of personal data – the data controller. However, in case of violations of the main principles of national Privacy Act by the processor with its registered seat outside of Bosnia and Herzegovina, DPA is entitled to take necessary steps through international co-operation with competent DPA authorities.

The Privacy Act shall apply to personal data that are processed by all public authorities, natural and legal persons, unless otherwise stipulated by other legislation. The Privacy Act shall not apply to personal data being processed by natural persons exclusively for personal needs and to accidental personal data collection, unless these data are subject to further processing.

IMPORTANT DEFINITIONS

4

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 in the Privacy Act as "any information relating to an identified or identifiable natural person". Personal data that identify a citizen are called identification data (name, address, date of birth etc.). Based on the legal definition, it can be reasonably concluded that if an individual cannot be identified because the data about him are in such form that does not allow identification (such as strong encryption where the provider does not possess the encryption key and thus is not in a position to decrypt the data), the data would most likely not be considered personal data.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

Yes. The Privacy Act defines special categories of data as any personal data revealing:

(i) racial origin, nationality, national or ethnic origin, political opinion or party affiliation, trade union affiliation, religious, philosophical or other belief, health, genetic code, sexual life;

(ii) criminal conviction, and

(iii) biometric data.

In principle, processing of special categories of personal data is prohibited. However, there are exemptions and processing would be allowed:

(i) if a data subject has explicitly granted his/her consent;

(ii) if the data processing is necessary to protect the life and health, property and other vital interests of the data subject or some other person for whom such consent cannot be obtained, in particular, when physically, mentally or legally incapacitated person is concerned, or if the person concerned is missing or for other similar reasons;

(iii) if the data processing is necessary for the fulfilment of an obligation or exercise of special rights of the controller arising from the labor legislation, to the extent the controller is authorized by law to such processing;

(iv) if the data processing is carried out to serve the needs of preventive medicine, medicinal diagnostics, the provision of medical care or the management of health care services, provided that such data are processed by a health professional obligated to maintain professional secrecy under the law or code of conduct of the responsible authority, or by other persons who are also subject to an equivalent obligation of secrecy;

(v) if the data processing is carried out within the scope of legitimate activities of an institution, foundation, association or any other non-profit organization with political, philosophical, religious or trade union objectives, provided that the data processing solely relates to the members of the bodies or persons who have regular contacts with them in connection with their objectives and that the data are not disclosed to a third party without the consent of the data subject;

(vi) if the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims;

(vii) if it is of special public interest or in other cases stipulated by law; in such cases the law shall provide appropriate protection mechanisms.

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

6

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

The Privacy Act and other data protection regulations do not specifically address matters related to cloud computing. In the context of cloud computing, the cloud provider will in most cases be the data processor while the cloud customer will be the data controller. According to the Privacy Act, the processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (e.g. cloud service provider). The processor acts only on the basis of the controller's instructions and in accordance with the provisions of the Privacy Act and is responsible for personal data processing according to the data controller's instructions.

The Controller is defined as any public authority, natural or legal person, agency or any other body, which, independently or together with another

party, manages, processes and determines the purpose and the manner of personal data processing on the basis of laws or regulations (e.g. local company). The controller is required to: process personal data fairly and lawfully; process personal data collected for special, explicit and lawful purposes in no manner contrary to the specified purpose; process personal data only to the extent and scope necessary for the fulfilment of the specified purpose; process only authentic and accurate personal data, and update such data when necessary; erase or correct personal data which are incorrect and incomplete, given the purpose for which the data are collected or further processed; process personal data only within the period of time necessary for the fulfilment of the purpose of their processing; keep personal data in a format that allows identification of the data subject for no longer than required for the purpose for which the data are collected or further processed; ensure that personal data that were obtained for various purposes are not combined or merged. Furthermore, the controller shall be required to check whether the personal data are authentic and accurate. If the incomplete and inaccurate data cannot be corrected or amended, and considering the purpose for which they are collected or further processed, the controller must destroy them without delay.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes. The processor is required to conclude an agreement with the controller on personal data processing (Personal Data Processing Agreement), specifying the scope, purpose and the period of time for which the agreement has been concluded, as well as adequate guarantees of the processor in terms of technical and organizational protection of personal data.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

In principle, yes, but only when authorized by the data controller.

While exercising its duties, the processor (cloud provider) shall not transfer its responsibility to other (sub-)processors, unless explicitly instructed by the data controller to do so. The data controller, in turn, would have to be authorized by the data subject to engage a sub—processor, unless the data controller processes the personal data on legal grounds other than the explicit consent of the individual data subject. These alternative legal grounds for data processing and transfer to third parties include: when the processing/transfer is prescribed by law; if the transfer is required to fulfill the contract between the individual and the controller, or in order to fulfill the obligations and specific rights of the data controller in the field of employment; exceptionally, if the transfer of personal data is necessary for the achievement of statutory powers, duties and obligations of the public sector, provided that such treatment does not endanger legitimate interests of the individual to whom personal data relate; if that is necessary for the fulfillment of the legal private sector interests and those interests clearly go beyond the interests of individual institutions to which the personal data relates.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

The Privacy Act does not distinguish between transfers to EU and non-EU countries. A general principle under the Privacy Act is that personal data may not be transferred to countries that do not offer an adequate level of data protection.

Countries that are considered to offer an "adequate level of protection" are not listed but the DPA will decide if a particular country meets this criteria. According to the DPA's current practice, EU countries qualify while transfers to the USA are subject to severe restrictions. The adequacy of safeguards is estimated on the basis of the specific circumstances of

the transfer; in particular, the following criteria are taken into account:

(i) purpose and period of processing;

(ii) the country in which data is transferred;

(iii) statutory rules in force in the country in which data are transferred;

(iv) professional rules and security measures that must be respected in that country.

The DPA may approve the transfer of data from Bosnia and Herzegovina to another country which does not provide an appropriate level of protection provided that the data important in such third country provides adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals or provision of similar rights arises from the provisions of a special agreement.

Exceptionally, personal data may be transferred abroad if the data subject has given his/her consent with such transfer, when the transfer is necessary in relation to a contract or a legal claim, and when the transfer is necessary to protect the public interest.

10

What are the requirements to transfer personal data to a non-EU country?

The Privacy Act does not distinguish between transfers to EU and non-EU countries. The criteria for cross-border transfer are determined in the basis of the adequacy of data protection in the recipient country, as assessed by the DPA. Please refer to the previous question.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

Yes. Controllers and processors are obliged to take measures against unauthorized or accidental access to personal data, alteration, destruction or loss of data, unauthorized transmission, other forms of unlawful processing of data, as well as measures against the misuse of personal data. This obligation remains in effect even after the completion of data processing. The controller and, within its competence, data processor, are required to make a plan for data security (safety plan), which is determined by technical and organizational measures for the security of personal data. The Privacy Act, however, does not further specify the measures; however, the measures are elaborate in the Regulation on Keeping of the Personal Data and Specific Measures on Technical Protection of Personal Data (see next question).

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

While the law does not regulate cloud computing specifically, the Regulation on Keeping of the Personal Data and Specific Measures on Technical Protection of Personal Data („Official Gazette of Bosnia and Herzegovina“ 67/09), which is a bylaw issued under the Privacy Act, would be applicable to cloud providers as processors. This Regulations provides for the following key security measures that must be contained in the Safety Plan:

(i) organizational measures, such as informing and training of personnel working on the personal data processing, physical measures of protection of working premises and equipment related to personal data processing, prevention of unauthorized duplication, copying or transcribing of personal data, destroying of personal data etc.

(ii) technical measures such as control of access to premises and equipment for personal data processing, protection from destroying and damaging of personal data, etc.

OTHER REQUIREMENTS

13

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

No. Personal data must be processed only in the necessary scope and for the purposes for which they were collected and not further processed in a way incompatible with those.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

Neither the Privacy Act nor the bylaws explicitly entitle the data controller (customer) to audit the data processor (cloud provider). However, relevant audit/inspection rights by the data controller of the data processor's operation can be regulated by the provisions of the data processing agreement between the parties.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

There is a general notification obligation applicable to all data controllers who must, prior to commencing any personal data processing, notify the DPA of the intended processing by filing a Notification of intention to establish a personal data filing system. The cloud customer (data controller) is thus required to notify the DPA and to obtain approval to use cloud services since cloud service provider is subject to the same requirements as any other data processor.

PUBLIC SECTOR

16

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

No. There are no different data protection requirements applicable to cloud customers from the private and the public sector.

FINANCIAL DATA

17

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 are no finance sector-specific rules applicable to cloud computing (or to outsourcing, generally).

18

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

No, there are no such notification or approval requirements other than the general notification requirement of intended personal data processing operations described in response to question 15 above.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

No, there is no guidance issued by the DPA or other relevant authorities on cloud computing specifically.

PENDING LEGISLATION

20

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

No, there is no pending legislation that may have significant impact on cloud computing.

GEORGIA

COUNSEL DETAILS:

Country: Georgia

Attorney: Mikheil Gogeshvili

Law Firm: Mgaloblishvili Kipiani Dzidziguri (MKD) Law Office
71 Vazha Pshavela Ave., Office 24, 0186 Tbilisi,
0186 Tbilisi
Georgia

Website: www.mkd.ge

E-mail: mgogeshvili@mkd.ge

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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

The Law of Georgia on Personal Data Protection (in Georgian: კანონი პერსონალურ მონაცემთა დაცვის შესახებ), dated 28 December 2011 (the "Privacy Act").

Unofficial English translation of the Privacy Act can be found at: http://personaldata.ge/res/docs/Kanoni/PDP%20Law.pdf

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or the "DPA")? Summarize its powers.

საქართველოს პერსონაღურ მონაცემთა დაცვის ინსპექტორი Office of the Personal Data Protection Inspector (in Georgian: საქართველოს პერსონაღურ მონაცემთა დაცვის ინსპექტორი) (hereinafter referred to only as the "DPA").

Address: 15 Apakidze str., Tbilisi, Georgia

Web: http://personaldata.ge/en/home

The DPA represents an independent administrative entity not subordinated to any governmental body but accountable to both the Parliament and the Government of Georgia. The DPA's authority encompasses the following broad competences:

(i) consulting public bodies, natural and legal persons on issues related to personal data protection;

(ii) overseeing compliance with personal data protection legislation by various stakeholders;

(iii) reviewing complaints and hearing appeals on alleged violations of personal data protection legislation;

(iv) conducting investigations (including on-site visits);

(v) application of administrative sanctions in case of violations of data protection legislation which constitute administrative offences under the Privacy Act;

(vi) granting approvals for trans-border flow of personal data;

(vii) maintaining the registry of filing system catalogues (holding records of the filing systems managed by various data controllers).

3

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

The Privacy Act applies to the processing of data on the Georgian territory (including at the Georgian diplomatic missions abroad) by automated or semi-automated means as well as to the processing of the data by non-automated means which form, or are intended to form, part of a filing system.

The Privacy Act also applies to the activities of a data controller who is not registered in the territory of Georgia but exploits technical means located in Georgia for data processing purposes, except when these technical means are used solely for the transit of data.

IMPORTANT DEFINITIONS

4

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 is defined as any information relating to an identified or identifiable natural person. A person will be regarded identifiable when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural or social features/factors specific to this person.

There is no conclusive guidance on the status of encrypted data but the Privacy Act does define "de-identification" as data modification that makes it impossible to link specific data to the relevant data subject. Hence, encrypted data may be regarded as "de-identified" and therefore not constituting personal data.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

The Privacy Act recognizes so called sensitive data which represents data connected to a person's racial or ethnic origin, political views, religious or philosophical beliefs, membership of professional organizations, state of health etc. Biometric data also falls in the definition of sensitive data.

Sensitive data must be processed on the basis of legitimate grounds prescribed by the Privacy Act and a data subject's written consent; the level of protection afforded to sensitive data is similar to the protection granted to other personal data.

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

6

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

Data controller is a public agency, natural or legal person who individually or jointly with others determines purposes and means of personal data processing and who, directly or through a data processor, processes personal data. Data processor is any natural or legal person who processes personal data for or on behalf of the data controller.

In the context of cloud services, the customer purchasing the services is usually deemed the data controller while the cloud service provider is deemed a (mere) data processor.

Primary obligations of the data controller include:

(i) provide data subject with information regarding identity of the data processor, nature of data being processed, purpose of data processing;

(ii) not to engage a data processor who is likely to misuse personal data;

(iii) monitor the processing of personal data by the data processor;

(iv) interact with the DPA when data processing activities require notifications to or approvals by the DPA.

Primary obligations of the data processor include:

(i) process data within the scope and in conformity with the purpose determined, e.g. in the agreement concluded with the data controller;

(ii) implement relevant organizational and technical measures to protect the personal data that is being processed;

(iii) not to subcontract data processing activities without the data controller's consent;

(iv) cease the processing and return to the data controller any data received prior to the termination of its processing authority.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes, an agreement between a customer and cloud provider is required. The Privacy Act does not prescribe its minimum content except for the requirement that the agreement should include the data processor's obligations with respect to the measures related to personal data security.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Yes, subject to the data controller's consent. The data controller should not engage a data processor who, given the latter's profile (e.g. the nature of the data processor's professional activities) is likely to misuse the personal data. No other statutory conditions apply.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

The Privacy Act provides for an unrestricted transfer of personal data to countries which are specifically "whitelisted" pursuant to the Order N1 of the DPA dated 16 September, 2014. All EU Member States are "whitelisted".

10

What are the requirements to transfer personal data to a non-EU country?

Intended data transfers to countries not listed in the Order N1 (such as, for instance, the USA) are subject to the DPA's prior approval.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

The Privacy Act does not elaborate on specific technical or organizational measures; rather, it provides for a general obligation of the data controller to implement appropriate organizational and technical measures to ensure the protection of data against accidental or unlawful destruction, alteration, disclosure, collection or any other form of illegal use, as well as accidental or unlawful loss thereof.

In addition, data controllers should maintain logs of all operations performed in relation to electronic data.

In case of data disclosure, the data controller and data processor must keep records of the following information: the specific data that was disclosed, to whom such data was disclosed, and when and on what legal grounds such data was disclosed. This information must be stored together with the data on a data subject it relates to for the entire (applicable) storage period.

12

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

No.

OTHER REQUIREMENTS

13

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

No. Under the Privacy Act, personal data may be processed only for predetermined, specific, clearly defined and legitimate purposes. Data processing for purposes that goes beyond and/or is incompatible with the original purpose or scope is therefore inadmissible.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

While the Privacy Act generally provides for the customer's right to monitor the processing of his personal data, it does not explicitly regulate the latter's audit right. In the absence of any restrictions, however, the parties are in principle authorized to: (i) include the customer's audit rights in their contract; and (ii) agree to an audit by an independent auditor nominated by the cloud provider.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

Apart from the general notification obligation of data controllers towards the DPA prior to the establishment of the personal data filing system (including subsequent notifications on additional entries of personal data in the respective filing system), and apart from the DPA's approval

required for data transfers to non-whitelisted countries (see questions 2 and10, respectively), the use of cloud computing services in itself is not subject to any specific notification or approval.

PUBLIC SECTOR

16

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

No. The Privacy Act does not distinguish between public and private sector data controllers (a data controller is defined as any public or private institution, entity or natural person). Hence, the same statutory requirements generally apply to cloud customers from both private and public sector.

FINANCIAL DATA

17

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.

Order N 47/04 of the National Bank of Georgia on Managing Operational Risks by Commercial Banks, dated 13 June 2014 ("NBG Order 47/04") regulates, among other things, requirements applicable to information technologies as well as outsourcing by commercial banks of their banking activities (and related information systems/technologies).

NBG Order 47/04 provides that commercial banks must employ policies and procedures that address the adequacy and security of their information systems which, in turn, should be based on recognized international standards (such as NIST or ISACA). Banks should regularly conduct information systems audits. Audits may be carried out either by internal audit units or external, recognized auditors.

Outsourcing agreement must provide for the authority of NBG to receive any information pertaining to the activities of a commercial bank.

Use of a foreign-based third-party service provider and the location of critical data and processes outside Georgia must not deprive or restrict NBG's ability to access or examine the commercial banks' banking operations. Outsourcing of the services to jurisdictions where full and complete access to information may be impeded by various legal or administrative constraints will be particularly sensitive and not acceptable.

18

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

Commercial banks should notify the NBG the details of the planned outsourcing arrangement. Within 30 business days of receipt of the notification (with a possible additional 30 day extension period), the NBG approves or disapproves the outsourcing arrangement. An outsourcing agreement which is not approved by the NBG is deemed invalid.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

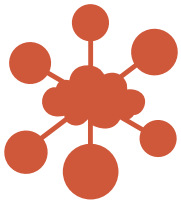
No. The DPA has not issued any guidance on cloud computing specifically.

PENDING LEGISLATION

20

Is there any pending legislation that will have significant impact on cloud computing?	No.

KAZAKHSTAN



COUNSEL DETAILS:

Country: Kazakhstan
Attorney: Zhibek Aidymbekova
Law Firm: Norton Rose Fulbright (Kazakhstan) Limited
Manas Street 32A
050008 Almaty
Kazakhstan
Website: www.nortonrosefulbright.com/ka
E-mail: zhibek.aidymbekova@nortonrosefulbright.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

The statutory basis for the protection of personal data in Kazakhstan is the Law of Kazakhstan No. 94-V "On Personal Data and Its Protection" dated 21 May 2013 (the "Privacy Act") (In Russian *"Закон Республики Казахстан* № 94-V *''О персональных данных и их защите" от* 21 *мая* 2013 *года")*, which became effective on 25 November 2013. The Privacy Act is not substantially identical with the EU Data Protection Directive.

The official Russian version of the Privacy Act is available at: http://adilet.zan.kz/rus/docs/Z1300000094, however, there is no official English version of the Privacy Act available.

Essentially, the Privacy Act is designed to regulate collection, processing and protection of personal data, and defines the fundamental principles and legal basis for such activity.

In addition there are several Decrees of the Government of Kazakhstan (the "Government") adopted in order to further clarify the requirements set out by the Privacy Act.

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or the "DPA")? Summarize its powers.

There is no special data protection authority appointed by the Privacy Act. Instead, the overseeing responsibilities are split between:

(i) the Government ("Pravitelstvo Respubliki Kazakhstan"

(http://government.kz/index.php/en/) and

(ii) (ii) various state authorities (to the extent their activities are related to the data protection queries) including, but not limited to, the Prosecutor's Office ("Generalnaya Prokuratura", 14, Orynbor Street, Astana, 010000, Kazakhstan; http://prokuror.gov.kz/eng).

The Government is entitled to develop the main data protection regulations and to approve procedures for protecting personal data by an owner and/or an operator or any third party. It is also within the Government's competence to oversee other state authorities.

The state authorities are entitled to receive and consider complaints from individuals and legal entities regarding alleged violations in the area of data privacy protection and undertake enforcement for such violations.

The Prosecutor's Office representing Kazakhstan is in charge of supervision over precise and uniform compliance with the Privacy Act. In addition, the Prosecutor's Office is authorized to provide the official interpretation of Kazakhstan legislation upon request of the state authorities.

Ministry of Health and Social Protection of Kazakhstan ("Ministerstvo Zdorovya I Sotsialnoj Zaschity", 8, Orynbor Street, Astana, 010000,

Kazakhstan; http://mzsr.gov.kz; email: minzdravsoc@mzsr.gov.kz) is in charge of the matters involving personal data disclosure in the area of employment and medical aid services.

Ministry of Industry and Development of Kazakhstan ("Ministerstvo Industrii i Razvitiya", 8, Orynbor Street, Astana, 010000, Kazakhstan; http://www.mk.gov.kz/eng/index.php; email: mid@mid.gov.kz) for improper use of electronic information resources that cause property or moral damage to the personal data owners.

3

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

The Privacy Act applies to personal data owners, database owners and operators (see question 6 for definitions) which deal with collection and processing of the personal data. The Privacy Act does not expressly state as to whether database owners and/or operators shall be established in Kazakhstan; however, the purpose of collecting personal data of such owners and operators shall be in strict compliance with Kazakhstan laws (e.g. mandatory collection of information by employers).

The term "personal data" is defined, quite broadly, as the "data on a particular subject or allowing identifying the particular subject stored on the electronic, paper, and/or other material data holder". Therefore any use of the cloud by the individuals ("subjects") should fall under the regulation of the Privacy Act.

The Privacy Act sets out the exhaustive occasions where it does not apply. The only exemption the cloud services providers may rely on is "the collection, processing and protection of the personal data solely for personal and family needs, if it does not violate the rights of other individuals and (or) legal entities and the requirements of the laws of Kazakhstan;"

Therefore any personal data regarding (i) any individual within Kazakhstan and (ii) Kazakhstan individuals globally is subject to regulation of the Privacy Act including where such information is subject to cloud services arrangements.

IMPORTANT DEFINITIONS

4

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?

The Privacy Act defines "personal data" as "information, stored on an electronic, paper and/or on other data holder, relating to an identified or identifiable individual".

Kazakhstan legislation does not contain a proper definition of the encrypted data. This leaves the room for interpretation for the state authorities which may qualify data stored by a cloud services provider which does not have access to the encryption key as personal data.

The Privacy Act addresses encryption as a technical measure of protection of personal data from unauthorized or accidental access, destruction, modification, blocking, copying, distribution of personal data, as well as other illegal actions.

The owner of the database containing personal data and/or the operator of the database containing personal data are mandatorily required to take all necessary measures, including the technical, in general, and cryptography, which may or may not include encryption, in particular, in order to protect the personal data from any illegal actions as set out above. For definitions of a "database owner" and "database operator", refer to question 6.

As per the Privacy Act the information relating to any particular or otherwise identifiable individual shall cease to qualify as "personal data", provided that such information is:

(i) anonymized; or

(ii) deleted.

Under the Privacy Act the "anonymized data" is the data which does not lead to the identification of an individual and such identification is impossible in principle. Further, the data shall be considered as destroyed if such data ceases to exist.

Therefore, based on the above, and despite the fact that the EU Data Protection Regulation provides that the data protection principles should not apply to the data rendered anonymous in such a way the data subject is no longer identifiable, the encrypted data may constitute "personal data" from the perspective of Kazakhstan legislation.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

Yes. The Privacy Act differentiates two categories of personal data and correlating level of protection. The basis of this differentiation is not the content of the data, but more the manner and terms of its accessibility.

Publicly available personal data shall constitute personal data with free access, provided that such access is approved by the individual to whom such data relates, or personal data which does not fall under the confidentiality regime prescribed by the Kazakhstan laws.

Personal data with limited access shall constitute personal data access to which is limited by the Kazakhstan laws.

The EU Data Protection Directive determines the data, concerning, inter alia, health or sex life as "sensitive information which can only be processed either (i) with the explicit consent of the data subject, or, (ii) without such consent only if one of the specific conditions stipulated in the EU Data Protection Directive is met. Kazakhstan Health Code[1] establishes a similar regime stipulating that the fact of application for medical assistance and health conditions report is "medical secret". It is prohibited to distribute or publish any such personal data without the prior consent of the individual or in cases specifically stipulated by the Health Code, i.e. if the individual is unable to express his will, threat of epidemics, court decision and disputes. From the perspective of the Privacy Act the health data is of a personal data with a limited access.

1 The Code of Health of People and Healthcare System dated 18 September 2009 (In Russian – *Кодекс Республики Казахстан* №193-IV *"О здоровье народа и системе здравоохранения" от 18 сентября 2009"*)

According to the Privacy Act the database owner and/or the database operator, as well as any third parties having access to personal data with a limited access, shall ensure the confidentiality of such data and preclude disclosure thereof in any form without the consent of the individual to whom such personal data relates, except for certain cases when the disclosure of such data is allowed by the Kazakhstan laws without the prior consent of the individual.

Formally, any individual, who became aware of the personal data with limited access due to their professional activity or based on the employment relations, shall ensure the confidentiality of the received data.

Based on the above, essentially, the crucial difference between publicly available personal data and personal data with a limited access is that the latter shall always remain confidential and may only be disclosed to third parties with the relevant consent of the individual to whom it relates or on narrow grounds specifically stipulated by the Kazakhstan legislation.

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

6

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

The Privacy Act does not contain definitions of "data processors" and "data controllers". Instead, it contains definitions of the "database operator" and "database owner".

Database owner is a public authority, a legal entity or an individual, which uses, possesses and disposes personal data. The database operator is the public authority, a legal entity or an individual carrying out activities concerning collection, processing[2] and protection of personal data. Thus, cloud services providers would be treated as the database operator, while its cloud service clients will be considered the database owners.

2 For the purposes of the Privacy Act, those cover each of storage, accumulation, use, distribution and deletion

The database owners and operators key obligations and competencies under the Privacy Act include the following:

(i) approve the list of personal data, necessary and sufficient to undertake their tasks, unless otherwise provided by the laws of Kazakhstan;[3]

(ii) adopt legal, organizational and technical measures that are necessary for the protection of personal data in accordance with the legislation of Kazakhstan;

(iii) comply with the legislation of Kazakhstan on personal data and its protection;

(iv) delete personal data if the purpose of its gathering and processing has been achieved, as well as in other cases stipulated by the Privacy Act and other legislative acts of Kazakhstan;

(v) store the data subject's consent with the collection and processing of personal data in the cases provided for by the legislation of Kazakhstan;

(vi) provide information relating to the processing of personal data of a data subject, within three business days of receipt of the request for information from the subject or his/her legal representative, unless other period is stipulated in the laws of Kazakhstan, or provide a reasoned response when such information is not provided;

(vii) within one business day:

a. revise or amend the personal data as per relevant documents confirming their authenticity, or delete personal data if it cannot be revised or amended;

3 Please note that the criteria or necessity and sufficiency are not at the discretion of the database and owners – there is a specific governmental decree addressing the minimal limitations to such criteria.

b. block personal data related to the data subject in case of a confirmed violation of the terms on the basis of which the data has been collected;

c. delete personal data if, pursuant to a decision of an authorized state body, its collection or processing violates the law;

d. unblock the access to personal data if no violation of the data processing rules has been established terms on the.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

The Privacy Act does not mandatorily require a formal agreement between a customer and a cloud services provider. However, the rights of the subject of personal data as well as obligations of the cloud services provider should be addressed in the relevant agreement between the customer and the cloud services provider, including, inter alia, a provision that the cloud services provider may only act on the instructions of the customer.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

The Privacy Act does not establish a restriction to use sub-processors, therefore, it can be reasonably concluded that sub-processing is not restricted. However, requirements which apply to the cloud services provider most likely will be applicable to the sub-processors as well and it would be advisable to obtain a prior consent of the customer before engaging any sub-processors.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

As a general rule, any collection and processing of personal data, including its transfer, shall be subject to consent of the individual to whom such data relates.

Under the Privacy Act personal data may be transferred to any foreign country (regardless whether it is an EU country or a non-EU country), provided that such foreign state-recipient of personal data shall ensure an adequate protection of the transferred personal data, which includes protection against an unauthorized or accidental access, destruction, modification, blocking, copying, distribution of personal data, as well as any other illegal actions.

The Privacy Act does not provide any guidance on the adequacy of the data protection to be afforded by such foreign country recipient of personal data. With regard to transfer of personal data to EU countries, it can be reasonably concluded that an EU country can be considered a country with the adequate level of protection of personal data if it is, at least, a member of the 1981 Council of Europe Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, which imposes certain requirements for the protection of personal data.

The Privacy Act further provides that cross-border transfer of personal data to foreign countries which does not ensure an adequate protection of personal data, can be carried out if:

(i) a consent of an individual to whom such data relates is obtained;

(ii) it is provided by international treaties ratified by Kazakhstan;

(iii) it is stipulated by Kazakhstan laws as necessary to protect the constitutional order, public order, the rights and freedoms of a man and a citizen, public health or moral rules; and

(iv) it is necessary to protect constitutional rights and freedoms of a man and a citizen, while obtaining of the consent of an individual to whom such data relates is not possible.

10

What are the requirements to transfer personal data to a non-EU country?

The Privacy Act does not differentiate between EU or non-EU countries. Please see the response to question 9.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

The Privacy Act generally obligates the database owners and operators to implement and observe necessary measures, including legal, organizational and technical, for protection of personal data, however, it does not further specify these measures.

These measures are generally defined in the Law of Kazakhstan No. 217-III "On Informatization" dated January 11, 2007 (the "Informatization Law") (In Russian "*Закон Республики Казахстан* №217-III "*Об информатизации" от* 11 *января* 2007 *года*") as outlined in question 12 below.

12

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Under the Informatization Law any electronically stored information (databases) containing personal data are qualified as confidential electronic resources. Protection shall be ensured through the following measures:

(i) Legal measures: through agreements between owners or possessors of the resources with users of information (i.e. cloud service customers), which contain terms and conditions regarding the access and use of certain information resources, including, among others, liability provisions for breach of such conditions;

(ii) Organizational measures: through a special access regime for facilities where the information is stored, and through establishing limitation of access to information based on the various factors such as persons and type of information; and

(iii) Technical measures: through physical protection of information systems, use of cryptographic protection and introduction of access control and registration.

These measures shall be undertaken by any owners, possessors or operators in the area of informatization, which may (and will likely) include cloud services providers.

OTHER REQUIREMENTS

13

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

No, it would not be permissible. Personal data must always be collected for specified purposes and not further processed/used in a way incompatible with those purposes.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

The Informatization Law provides the owners and/or possessors of information systems with the right to initiate the audit of such systems. Such audit must be conducted by a person/entity which has special knowledge and experience in the IT area. The cloud users, providing the data to the cloud, will therefore have the right to initiate the audit of a cloud data centre. The parties may agree to an audit by an independent auditor (expert company) selected by the cloud provider.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

No notification or approval from the regulators is required for a customer to use a cloud service.

PUBLIC SECTOR

16

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

No, there are no such requirements in the publicly available regulations.

FINANCIAL DATA

17

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 are no such sector-specific requirements in the publicly available regulations.

18

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

There are no such notification or approval requirements in the publicly available regulations.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

There is no further publicly available guidance on cloud computing issued by the data protection authority or any other relevant authority in Kazakhstan.

PENDING LEGISLATION

20

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

Yes. A legislative act that would amend, inter alia, the Privacy Act, is currently being reviewed by the Parliament As the draft of the amendment is not publicly available, it is unclear what changes are being proposed and whether they will have any impact on cloud computing.

Further, Kazakhstan adopted the State Program (Concept) "Informational Kazakhstan-2020" by the Order of the President of Kazakhstan dated 8 January 2013 (the text of the document in Russian can be found at: http://www.adilet.zan.kz/rus/docs/U1300000464), which indicates the necessity for further development of information technologies in Kazakhstan, including cloud services. It can be anticipated that this initiative will eventually result in the adoption of legislation regulating data protection in the context of new information technologies and concepts such as cloud services.

MACEDONIA

COUNSEL DETAILS:

Country: MACEDONIA
Attorney: Prof. Dr. Valentin Pepeljugovski
Law Firm: Law Office PEPELJUGOSKI
"Veljko Vlahovik" 4/1-1
1000 Skopje
Republic of Macedonia
Website: www.pepeljugoski.com.mk
E-mail: vpepeljugoski@unet.com.mk

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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Law on Personal Data Protection of 2005 (*„Закон за заштита на личните податоци"*), published in the Official Gazette of the Republic of Macedonia no. 7/2005, as amended (Official Gazette of the Republic of Macedonia 103/2008, 124/2008, 124/2010, 135/2011, 43/2014) (the "Privacy Act"). The Privacy Act is to a large extent modeled upon the EU Data Protection Directive.

Other legislative acts include: The Law on Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Rules on the Technical and Organizational Measures for Providing Secrecy and Protection of the Processing of Personal Data, Rules on the Notification of the Personal Data Collection and Storage and Notification to the Central Register of Data Processing, Rules on the

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or "DPA")? Summarize its powers.

Transfer of data, Guidelines for the Internal and External control of the Information System etc.

An English version of the Privacy Act is available at http://www.dzlp.mk/sites/default/files/Law_on_Personal_Data_Protection_Cleared_version_0.pdf

---

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or the "DPA")? Summarize its powers.

Дирекција за заштита на лични податоци ("Directorate for personal data protection", hereinafter referred to only as the "DPA")

Address: Blvd. "Goce Delcev" 18 (Building of the Macedonian Radio Television – 14th floor), Post Office box 417 1000 Skopje; http://dzlp.mk/en

The DPA is the central authority that oversees compliance with data protection law. The DPA is managed by a Director, appointed and dismissed by the Assembly of the Republic of Macedonia upon the proposal of the Commission for Election and Appointment Matters of the Assembly of the Republic of Macedonia.

The main competencies of the Directorate are: prepare and adopt by-laws relating to personal data protection; develop policies and give directions related to personal data protection; perform inspection and supervision in accordance with the provisions of the Privacy Act (on a regular as well as ad hoc basis); assess the fairness and legality of the personal data processing; keep a Central Register of data processing, issue prior approval for personal data processing in accordance with the Privacy Act; issue decisions prohibiting controllers from further processing of personal data; issue approvals for personal data transfer to other countries; opine on draft regulations and codes of conduct in the field of personal data protection; conduct misdemeanor proceedings; cooperate with foreign data protection authorities; conduct trainings ; participate in the work of the international organizations and institutions for personal data protection; and perform other activities determined by law.

3

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

The Act does not explicitly stipulate this; however, it is applicable to all entities that operate on the territory of the Republic of Macedonia. The applicability of local law is triggered by the place of establishment of the entity that is responsible for the processing of personal data – the data controller.

IMPORTANT DEFINITIONS

4

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 is defined as "any information pertaining to an identified or identifiable natural person, an identifiable entity being an entity whose identity can be determined directly or indirectly, in particular on the basis of the personal identification number of the citizen or on the basis of one or more characteristics, specific for his/her physical, mental, economic, cultural or social identity".

There is currently no conclusive decision or guidance on when encrypted data may be safely regarded as anonymized data and thus outside of scope of personal data protection.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

Yes. The Privacy Act defines "special categories of personal data" as personal data revealing the data subject's racial or ethnic origin, political views, religious or other beliefs, membership in a trade union, and data relating to the health condition of the data subject, including genetic data, biometric data or data referring to the sexual life.

Special categories of personal data may only be processed in the following cases:

(i) on the basis of an explicit consent of the personal data subject unless the law provides otherwise;

(ii) if it is necessary for performing specific rights and obligations of the controller in the field of labor law, to the extent permitted by law;

(iii) when it is necessary for the protection of the essential interests of the data subject or of other person physically disabled to give consent or lacking the capacity to give consent;

(iv) if the processing is carried out in the framework of the activities of institutions, associations or any non-profit institutions for political, religious, trade-union or other purpose (subject to further limitations);

(v) when the processing concerns data which the data subject had publicly disclosed; (vi) when it is necessary for the purpose of determining or fulfilling individual legal interests of the data subject;

(vii) when it is necessary for the purpose of acquiring, exercising and protecting the rights of the data subject in a procedure with competent bodies;

(vii) if it is needed for the purposes of medical prevention, diagnosis, treatment or management of a public health institution and the processing is carried out by a person whose profession is to provide medical protection under oath of secrecy and proper measures for protection of public interest determined by law or decision of the DPA are implemented.

Otherwise, the Act does not differentiate between the treatment of sensitive personal data and regular personal data.

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

6

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

The Privacy Act defines a "controller of the personal data collection" as "any natural person or legal entity, a state administration body or other body, who, independently or together with others, determines the purposes and the ways of personal data processing" (hereinafter the "controller"). When the purposes and the ways of personal data processing are determined by law or any other regulation, the same law or regulation determines the controller or the special criteria for his/her selection.

The Privacy Act defines "processor of the personal data collection" as "a natural person or a legal entity or a legally authorized state administration body processing the personal data on behalf of the controller" (hereinafter the "processor").

In light of the above mentioned definitions, the cloud solution provider will usually be considered "data processor" while the 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". There may be situations, however, where the cloud provider may be considered data controller as well: for example, where the cloud provider would processes the entrusted data for its own purpose.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes. A data processing agreement must be executed between the data controller and the data processor before any data processing operation in the cloud is carried out. The agreement must be concluded in a written form and must include:

(i) the obligation of the processor to act solely in accordance with directions received from the controller;

(ii) the obligation of the processor to implement such technical and organizational measures that guarantee secrecy and protection of the personal data processed;

(iii) the manner in which the controller may inspect and test the protection measures and controls implemented by the processor.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Yes. The Privacy Act defines a sub-processor as a "third party, which shall be any natural person or legal entity, a state administration body or other body that is not a personal data subject, a controller, or a processor, and that is directly authorized by the controller or by the processor to process the data".

The Privacy Act requires the consent of the data subject in order for the data to be disclosed to such third party sub-processor(s). In addition, the data subject has the right to be informed about the type of the service subcontracted, the characteristics of current or potential sub-contractors, and shall be provided guarantees that these entities undertake to comply with the relevant data processing law. A contractual flow down of the relevant data processor's obligation under its contract with the cloud customer to the sub-processors must be ensured.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

Generally, personal data may only be transferred to countries that provide an adequate level of personal data protection. Member states of the European Union or the European Economic Area are deemed to provide an adequate level of personal data protection.

10

What are the requirements to transfer personal data to a non-EU country?

Personal data may only be transferred to non-EU/EEA countries if such countries provide an adequate level of personal data protection.

The DPA evaluates the level of protection provided by the recipient country on the basis of the nature of the data; the purpose and duration of the proposed processing operation(s); the country where the data shall be transferred; rule of law and safety measures existing in the recipient country.

If the European Commission determines that a third country does not provide an adequate level of data protection, after receiving the notification, the DPA shall issue a decision prohibiting personal data transfer to such country. Conversely, if the DPA determines that a third country fails to provide an adequate level of data protection, it shall immediately notify the European Commission and prohibit the controller from transferring the data.

If the state where the data are to be transmitted does not provide an appropriate level of personal data protection, the controller may not transfer the personal data to such country, subject to the following exceptions when the transfer may take place:

(i) the personal data subject gave an explicit consent to the data transfer;

(ii) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre contractual measures taken in response to the data subject's request;

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

(iv) the transfer is necessary for the protection of public interest or for public safety;

(v) the transfer is necessary for determining or fulfilling individual legal interests of the data subject;

(vi) the transfer is necessary in order to protect the life or the vital interests of the data subject;

(vii) the transfer is made from a public data register or a data register open to a person who can demonstrate legitimate, in the extent permitted by law.

The personal data transfer to countries which fail to provide at least the same level of personal data protection as in the Republic of Macedonia may only be performed after prior approval from the DPA, under the condition that the controller adduces adequate safeguards with respect to the protection of the personal data, privacy rights and freedoms of the personal data subject.

The DPA informs the European Commission and the supervision bodies for personal data protection of the EU member states about the approvals issued.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

Yes. The Privacy Act requires the controller and the processor to apply appropriate technical and organizational measures to protect personal data from accidental or unauthorized destruction, accidental loss, alteration, unauthorized disclosure or access, in particular when the processing includes transmission of the data over a network, as well as from any kind of unauthorized processing. The Privacy Act, however, does not specify the technical or organizational measures to be implemented; the Privacy Act merely requires that these measures are appropriate to the risks involved and the nature of the data being processed. The measures must be documented by the controller and the processor. Specifically, personal data may be transferred via electronic

telecommunications network only if protected by appropriate methods that render them unreadable during transit.

In addition, the controller and the processor must keep records of persons authorized to carry out data processing operations, including the name and surname of the authorized person, date of issuance and expiry of the authorization, and the scope of the authorization.

12

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Yes. There are several laws and bylaws that impose specific requirements and that may be relevant to cloud providers that are also providers of electronic communications networks or services: Law on Electronic Communications (Official Gazette of the Republic of Macedonia 39/14, 188/14), Law on Macedonian Academic and Research Network (Official Gazette of the Republic of Macedonia 124/10, 47/11, 41/14), The Rulebook for providing security and integrity of the public electronic communications networks and activities that operators should undertake in the case of breach of the security of personal information dated 15. 1. 2015.

OTHER REQUIREMENTS

13

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

No, it would not be permissible. 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.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

No. The law does not explicitly provide for an audit right.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

While the use of a cloud computing service specifically does not trigger any new notification obligation, there is a general notification obligation applicable to all data controllers who must, prior to commencing any personal data processing, notify the DPA of the intended processing.

The notification must include:

(i) name of the personal data collection;

(ii) name and address of the controller and his/her head office, i.e. address, as well as of the controller's representative, if any;

(iii) purpose or purposes of the processing,

(iv) legal basis of the processing;

(v) category or categories of the data subjects and personal data processed;

(vi) the users or the categories of users to whom personal data may be disclosed;

(vii) time period for keeping the personal data;

(viii) anticipated transfers of personal data abroad; and

(ix) description of technical and organizational measures implemented to enables the DPA to assess the adequacy of such measures.

The controller may start to process the data once it obtains a confirmation letter from the DPA. The controller must notify the DPA of any changes to the processing within 30 days of such change.

The following data processing operations are exempted from notification:

(i) the personal data are part of a publicly available personal data collection pursuant to law;

(ii) the personal data collection contains data of no more than ten employees with the controller's organization;

(iii) the processing of personal data of members of associations founded for political, philosophical, religious or trade-union purposes.

The DPA keeps an electronic Central Register of personal data collections (data processing operations notified and approved). The Central Register is publicly accessible.

PUBLIC SECTOR

16

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

No, the Privacy Act does not distinguish between the private and the public sector.

Specific law regulating electronic management applies to public sector entities; it does not impose, however, any cloud-specific requirements.

FINANCIAL DATA

17

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.

"Circular for safety of the information system of the bank", issued by the Central bank in 2005, and the "Decision for connection with the system of the Central bank", are the two main documents that govern the processing of financial data. The Circular requires banks to implement appropriate security systems and security control (physical, technical and administrative). The banks are further required to keep a record (information book) of all data that they process as part of their banking activities. The data shall be classified in categories business secret, official secret, public documents, internal documents, classified documents and assets, etc. The Circular also requires that the banks conduct a risk assessment and define possible threats to the secrecy of the information. The bank's management must appoint one or more persons responsible for the security of the information technology (OSI S); each bank should also have an IT Steering committee which shall assist the management with the creation of an IT security policy. The OSI S may be subject to internal and external audit in accordance with the Standards for the Professional Practice of Internal Auditing issued by the Institute for Internal Auditors (IIA) or by the Information System Audit and Control Association (ISACA). The banks are permitted to outsource their IT operations.

18

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

No, apart from the general notification of intended personal data processing required under the Privacy Act (see answer to question 15).

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

No. The DPA has not issued any guidance on cloud computing specifically.

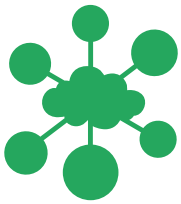
PENDING LEGISLATION

20

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

No. There is no pending legislation pertinent to cloud computing that is expected to be enacted in 2015.

MOLDOVA



COUNSEL DETAILS:

Country: Moldova

Attorney: Roger Gladei, Corina Vodă

Law Firm: Gladei & Partners
63 Vlaicu Parcalab Street (Sky Tower), Suite 5F2
MD-2012 Chisinau
Moldova

Website: www.gladei.md

E-mail: roger.gladei@gladei.md; corina.voda@gladei.md

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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Law on Personal Data Protection No. 133 of 08.07.2011 (the "Privacy Act"). The Privacy Act is modeled in line with the EU Data Protection Directive. Other privacy laws include: Law on Electronic Communications No. 241 of 15.11.2007, Law on Registers No. 71 of 22.03.2007, Law on Access to Information No. 982 of 11.05.2000, Law on Electronic Commerce No. 284 of 22.07.2004, Civil Code of the Republic of Moldova. The Privacy Act may be further supplemented by industry-specific rules.

An unofficial English version of the Privacy Act is available at http://datepersonale.md/en/legi/.

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or "DPA")? Summarize its powers.

Centrul Național pentru Protecția Datelor cu Caracter Personal ("National Center for Personal Data Protection", hereinafter referred to as the "DPA")

Address: Chisinau, MD-2004, 48 Serghei Lazo St.

Website: www.datepersonale.md

Email: centru@datepersonale.md

The DPA is an independent and autonomous public institution, empowered to perform control over compliance of personal data processing with the requirements of the Privacy Act and keep the register of personal data controllers. The DPA is entitled to authorize processing operations of personal data, carry out controls of the lawfulness of such processing and apply sanctions for breaches thereof.

3

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

The Privacy Act shall apply to processing of personal data performed by resident controllers (located on the territory of the Republic of Moldova) and diplomatic missions and consular offices of the Republic of Moldova. With respect to non-resident controllers, the Privacy Act shall apply to controllers situated in a place where the domestic law of the Republic of Moldova applies by virtue of international public law or controllers making use of equipment or other processing means situated on the territory of the Republic of Moldova, unless such equipment or means are used merely for transit purposes.

Personal data processing carried out exclusively for personal and family needs, processing of data constituting state secret, and processing operations and cross-border transmission of personal data referring to perpetrators or victims of genocide, crimes against humanity and war crimes, are exempted from the application of the Privacy Act.

IMPORTANT DEFINITIONS

4

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 any information related to an identified or identifiable natural person ("personal 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.

Neither the Privacy Act nor any other data protection regulations deal with the regime and status of encrypted data. Based on the current practice of the DPA, it can be reasonably concluded that encrypted data will not be considered personal data when the cloud provider does not possess access to the encryption key, unless such data is accompanied by other personal data which would allow identification of natural persons.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

Yes. The Privacy Act distinguishes between "personal data" and "special categories of personal data", the latter being defined as ''data revealing racial and ethnic origin, political opinions, religious and philosophical belief, social belonging, data concerning health or sex life, as well as relating to criminal convictions, administrative sanctions or coercive procedural measures".

Processing of sensitive data is possible only in the cases stipulated by the Privacy Act (e.g. the personal data subject has given his/her consent; processing is necessary for specific purposes such as employment, protection of the personal data subject's life, physical integrity or health, defense in a court of law, ensuring national security; processing relates to data which are voluntarily and manifestly made public by the personal data subject or is carried out for legitimate purposes by a foundation, association or any other non-profit organization in relation to its members. The Privacy Act regulates in detail sensitive data such as health-related personal data, data related to criminal convictions, coercive procedural measures or administrative sanctions and identifying data.

For instance, processing of health-related data may be carried out also when processing is required for purposes of preventive medicine, medical diagnosis, care or treatment of the personal data subject, or management of healthcare services employed in the interest of the personal data subject. Further, health-care professionals, healthcare institutions and their medical staff may process health-related personal data without the authorization of the DPA, provided that such processing is necessary to protect the personal data subject's life, physical integrity or health.

Personal data related to criminal convictions, coercive procedural measures or administrative sanctions may only be processed by or under the control of public authorities, within the limits of their competences and on the conditions laid out in the respective laws.

Generally, processing of special categories of personal data requires increased levels of security.

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

6

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

In a cloud computing context, the data controller is typically the customer of cloud computing services and the cloud provider is the data processor. Depending on the circumstances, however, the cloud provider may be deemed a joint data controller or a data controller in its own right, in particular should it process the data for its own purposes. Data controllers are bound under the Privacy Act to ensure the confidentiality of personal data and ensure appropriate technical and organizational measures to protect such data. They must also choose processors that are able to provide sufficient guarantees with respect to the technical and security measures required for processing of personal data. In turn, data processors are bound to act only on instructions from the controller and assist the latter in complying with data subjects' rights.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes. The carrying out of processing through a processor must be governed by a contract or other legal act, which shall stipulate in particular that:

(i) the processor shall act only on instructions from the controller; and

(ii) the controller shall implement appropriate technical and organizational measures to protect personal data against destruction, alteration, blocking, copying, disclosure and against other unlawful forms of processing, that shall ensure a level of security appropriate to the risks represented by the processing and the nature of data.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

The Privacy Act neither expressly regulates nor prohibits the appointment of sub-processors, although it refers to "persons who under the direct authority of the controller or the processor, are authorized to process personal data". Although the current practice of the DPA is to refuse the use of sub-processors, the DPA can generally be persuaded to permit such arrangement when the sub-processors are appointed with the consent of the data controller (typically, the data controller would appoint both the data processor and the sub-processor in the data processing agreement concluded between the data controller and the data processor). In any case, the data controller must be allowed to object to the use of sub-processors by the data processor.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

The Privacy Act's rules on cross-border transfer of personal data do not make distinction between transfers to EU and non-EU states. Generally,

cross-border transmission of personal data undergoing processing or intended for processing after transfer may take place only with the prior authorization of the DPA and only if the state in question ensures an adequate level of protection of the personal data and of the personal data subjects' rights.

As EU countries are deemed by the DPA to ensure a sufficient level of protection of the personal data and the personal data subjects' rights, no DPA authorization is required for the transfer of the data to EU countries.

10

What are the requirements to transfer personal data to a non-EU country?

The Privacy Act does not distinguish between transfers to EU and non-EU countries. When the DPA establishes that the legislation of the recipient non-EU country ensures an adequate level of protection, no authorization is required for the transfer of the data to such countries.

Conversely, when the level of protection is deemed inadequate, the DPA will only authorize the transfer of personal data provided that the controller offers sufficient guarantees of protection (set forth in the contract between the data controller and the person on whose request the transfer is made), and the personal data subject consents to such transfer.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

A data processor (cloud provider) shall, inter alia:

(i) prevent unauthorized connection to and interception of personal data (e.g. by encryption);

(ii) eliminate unauthorized access to processed personal data (e.g. by use of special technical and program means);

(iii) prevent actions which would cause destruction, alteration to personal data or failures of the functioning of the cloud (e.g. by setting a control system of software security and by performing regular back-ups);

(iv) prevent intentional/unintentional actions of internal/external users, employees of the personal data holders which may cause destruction, alteration to personal data or failures of the functioning of the cloud (e.g. by developing an access schedule).

Further, the cloud provider shall implement a data security policy (which shall be revised at least once a year and be approved by the cloud provider's top management), appoint a compliance officer, and instruct staff on the requirements related to processing of personal data, including their confidentiality.

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

No, there are no laws or regulations addressing security requirements for cloud providers specifically.

OTHER REQUIREMENTS

13

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. Thus, customer data could only be used by the cloud provider for advertising purposes if: (i) the mining of data for

advertising is approved by the cloud customer; (ii) the cloud provider acts upon instruction of the cloud customer; and (iii) the personal data subject's consent with such mining is obtained. Notably, the personal data subject has the right to object at any time and free of charge, without justification, to the processing of personal data relating to him/her for the advertising/marketing purposes. In addition, the cloud customer or the cloud provider is obliged to inform the person concerned about the right to object to such operation before his/her personal data are to be disclosed to third parties.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

TThe Privacy Act does not expressly confer such right on the cloud customer, enabling parties to decide on the inclusion of an audit right in the data processing agreement or other instrument the cloud customer and the cloud provider are bound to conclude (see question 7).

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

While the use of a cloud computing service specifically does not trigger any new notification obligation, there is a general notification obligation applicable to all data controllers/data processors who must, prior to commencing any personal data processing, notify the DPA of the intended processing.

The cloud customer (or the cloud provider, on behalf of the cloud customer) must notify the DPA before carrying out the processing of personal data intended to serve a certain purpose. Each processing of a new category of personal data shall be carried out under a new notification. Furthermore, processing of several categories of personal data, deemed as "sensitive", shall be subject to prior mandatory verification by the DPA, which shall issue a decision on approval or refusal of authorization of such processing.

PUBLIC SECTOR

16

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

No. Generally, data protection requirements differ depending on the level of protection required for their processing, and not on the nature of the customer (public or private).

However, public entities (ministries, central and subordinated administrative authorities, etc.) must ensure hosting of new information systems, as well as migration of existing automated information systems, onto the Common Government Technology Platform (MCloud), implemented in 2014. This mandatory hosting requirement may practically limit the use of private cloud services by public sector customers.

FINANCIAL DATA

17

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 be deemed to constitute outsourcing of the bank's activities and operations, as provided for in the Law on Financial Institutions No. 550 of 21.07.1995 and the Resolution of the National Bank of Moldova ("NBM") No. 241 of 03. 10. 2011 (the "NBM Resolution"). The NBM Resolution specifically regulates the concept of outsourcing of a "materially important activity", which shall mean the type of activity subject to licensing and authorization, any other activity/operation of such importance, so that any difficulty or failure to carry out/perform them can lead to the bank's inability to continue its financial activity and/or comply with the provisions of the laws and other normative acts. The NBM Resolution does not specify whether or when the use of cloud computing by a financial institution would be deemed outsourcing of a materially important activity. It is likely that in many instances, cloud computing would be considered as

such. In such case, the following key requirements would apply to the deployment of cloud computing by financial institutions:

(i) deployment shall not affect the bank's activity, reputation, efficient risk management and internal control systems;

(ii) appropriate control and risk management policies and procedures shall be set up by the bank;

(iii) the outsourcing provider's performance shall be evaluated by the bank at least once a year, including its financial and operational standing, compliance with confidentiality and security requirements;

(iv) an independent audit of the outsourcing provider's activities and operations shall be conducted on a yearly basis (or at NBM's request) by an international audit company accepted by the NBM.

18

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

Yes. Where the use of cloud computing is deemed as outsourcing of a materially important activity, the financial institution shall first obtain the written permission of the NBM. The law does not provide any notification requirements for the cloud provider.

To obtain NBM's permission, the bank shall submit a request accompanied inter alia by a detailed description of the outsourced activities/operations, information related to the cloud provider, and the draft of the outsourcing contract. The contract shall set forth rules concerning:

(i) the bank's right to terminate the contract if deemed necessary by the NBM or by the bank itself, on grounds of necessity and proportionality;

(ii) the bank's permanent monitoring rights;

(iii) the detailed description of the parties' obligations in case of early termination of the contract to ensure continuity of the bank's activities, etc.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

Relevant authorities have not issued hitherto any guidelines on cloud computing.

PENDING LEGISLATION

20

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

There is currently no draft legislation that could significantly impact cloud computing.

MONTENEGRO

COUNSEL DETAILS:

Country: MONTENEGRO
Attorney: Dragan Corac
Law Firm: Vujacic Law Offices
56/2 Boulevard I. Crnojevica
81000 Podgorica
Montenegro
Website: www.lawoffice-vujacic.com
E-mail: dragan.corac@lawoffice-vujacic.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Personal Data Protection Law (*Zakon o zaštiti podataka o ličnosti*), published in the Official Gazette of Montenegro 79/08, 70/09, 44/12 (the "Privacy Act").

The Privacy Act is modeled in compliance with the EU Data Protection Directive.

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or "DPA")? Summarize its powers.

Agencija za zaštitu ličnih podataka i slobodan pristup informacijama ("Agency for Protection of Personal Data and free access to information", hereinafter referred to only as "DPA").

Address: Kralja Nikole no. 2

Email: azlp@t-com.me

Website: www.azlp.me

The DPA is an independent central administrative body empowered to oversee compliance with the Privacy Act.

The DPA is entitled to perform supervision over the protection of personal data in accordance with the Privacy Act; decide on requests for protection of rights; deliver opinions with regards to the application of the Privacy Act; give consent with regards to the establishment of personal data filing systems; monitor the application of organizational and technical measures for the protection of personal data and propose improvement of such measures; put forward proposals and offer recommendations for the improvement in the protection of personal data; deliver an opinion as to whether a specific way of personal data processing puts rights and freedoms of individuals at risk; cooperate with authorities responsible for supervising the protection of personal data in other countries; cooperate with competent state authorities in the process of development of regulations relating to protection of personal data.

3

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

The Privacy Act applies to data controllers who process personal data in the territory of Montenegro or outside Montenegro, where in accordance with international law regulations of Montenegro apply.

The provisions of this law also apply to a data controller whose seat or domicile is outside Montenegro if the equipment for processing of personal data is situated in Montenegro, unless such equipment is used only for purposes of transit through the territory of Montenegro.

In the circumstances referred to in previous paragraph, the controller shall designate a representative with the seat or domicile in the territory of Montenegro who shall be responsible for the application of this law.

IMPORTANT DEFINITIONS

4

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 in the Privacy Act as any information relating to an identified or identifiable natural person. A natural person is one who is identified or 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.

Since there is currently no decision or guidance in Montenegro on encrypted data and taking into consideration the definition of personal data, encrypted data shall not be regarded as personal data in case the cloud provider does not possess access to the encryption key.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

Yes. The Privacy Act provides for a specific data treatment of so-called "special categories of data" which means personal data concerning racial or ethnic origin, political, religious or other beliefs, social origin, trade-union membership, and data concerning health or sex life.

Special categories of data can be processed exclusively under specific conditions enumerated by Privacy Act. These data shall be distinctively designed and protected in order to prevent unauthorized access.

The processing of personal data relating to criminal offences, criminal or misdemeanor penalties or security measures may be carried out only by or under the supervision of the competent state authority, provided that measures to safeguard personal data are provided in accordance with the law.

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

6

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

According the Privacy Act, "processor of personal data" shall mean a public authority, public administration body, self-government or local administration authority, company or other legal person, entrepreneur of a natural person, who performs tasks concerning the processing of personal data on behalf of the controller, in accordance with the law.

"Processing of personal data" is defined as any operation which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, use, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, as well any other operation performed upon personal data.

Controller of a personal data filing system may be a state body, public administration, local government authority or local government, corporation or other legal entity, entrepreneur or individual who perform the processing of personal data pursuant to the law. The purpose and means of the processing of personal data are determined by the controller of personal data, unless they are required by law.

In light of the above definitions, a cloud customer would be the data controller, since he determines the purpose of the processing and decides on the delegation of all or part of the processing activities to an external organization (cloud provider).

Generally, a cloud provider would be considered a data processor who processes personal data on behalf of the customer (data controller). However, in some cases when the cloud provider processes personal data for its own purposes he will be considered as controller in its own right.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes. If the controller (cloud customer) wishes to entrust specific activities concerning processing of personal data to a processor (cloud provider), the parties must enter into a written data processing agreement The agreement shall stipulate mutual rights and obligations of the controller and the processor, including, in particular, the processor's obligation to act on the instructions of the controller.

The activities related to personal data processing may be entrusted only to the processor who meets the requirements for implementation of technical, personnel and organizational measures for protection of personal data in accordance with the Privacy Act.

The processor must destroy or return the personal data to the controller once it ceases the processing activities.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

The Privacy Act does not explicitly regulate the use of sub-processors. However, since it is not forbidden, it can be reasonably concluded that it is permissible for a data processor to entrust some or all activities related to the processing of personal data to sub-processors. Such sub-processing would have to be permitted and regulated by a contract concluded between the processor (cloud provider) and the controller of personal data (cloud customer), i.e. the controller would have to approve such sub-processing.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

Personal data may be freely transferred to member states of the EU and EEA, as well as countries which are included on the European Commission's list of countries that are deemed to provide an adequate level of personal data protection. No regulatory approval of the DPA is required in such cases.

10

What are the requirements to transfer personal data to a non-EU country?

Personal data may be transferred to a non- EU country only with the prior consent of the DPA.

The consent of the DPA is not required in cases where:

(i) The transfer of personal data is provided for by a separate law or an international treaty binding on Montenegro;

(ii) The data subject has given his prior consent to the proposed transfer and has been informed of possible consequences of data transfer;

(iii) The transfer is required for the performance of a contract between a legal or natural person and the data controller or the implementation of pre-contractual obligations;

(iv) The transfer is required in order to protect the life of the data subject or is in his interest;

(v) The transfer is made from a register or records which according to laws or other regulations are available to the public;

(vi) The data are transferred to countries which are included on the European Union list of countries with an adequate level of personal data protection;

(vii) The transfer is necessary on important public interest grounds, or for the establishment, exercise or defense of legal claims of the data subject;

(viii) The data controller concludes a contract stipulating adequate contractual obligations accepted by the Member States of the European Union, with a personal data processor from the third country;

(ix) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a legal or natural person.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

Yes. Generally, the data processor must implement technical, personnel and organizational safeguards to protect personal data against loss, destruction, unauthorized access, alteration, disclosure and abuse. The safeguards must be appropriate to the nature and character of the data processed taking into account the highest level of technology and the costs of implementation.

If the processing of personal data is done electronically, the controller is required to ensure that the information system automatically records users of personal data, the data that are processed, the legal basis for the use of the data, case number, time of log out and log in to the system and if applicable, the period of time for which the information about the user will not be available to the data subject.

The Privacy Act, however, does not further specify the measures.

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

There are no other laws or regulations dealing specifically with security requirements for cloud providers. However, there is a Law on Information Security *(Zakon o informacionoj bezbjednosti, "Sl.list Crne Gore 14/2010")*, which applies to state authorities, state administration bodies, local governments, legal entities with public authority and other legal and natural persons who have access to or are handling personal data. The information Security Law requires the implementation of measures ensuring physical protection, protection of data, and protection of the information system.

A Government Decree on measures of information security *(Uredba o mjerama informacione bezbjednosti)* published in the Official Gazette of Montenegro 58/10) which implements the Law on Information Security determines the extent of information security required. Please refer to Section 7.

OTHER REQUIREMENTS

13

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

No. If the cloud provider wished to mine the data for advertising or marketing purposes, it would require the data subject's consent.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

This issue is not regulated by any specific local legislation, thus, there is no such statutory right.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

There are no specific prerequisites for a customer to use cloud services. Therefore, only general recording and notification rules prescribed for data controllers shall apply. According to the Privacy Act, data controller shall keep records of personal data filing system he established. Prior to establishing a personal data filing system, the controller must submit this information to the DPA.

PUBLIC SECTOR

16

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

The Privacy Act applies to all data processors and data controllers, and does not prescribe any different data protection requirements for public sector data controllers.

The Law on Information Security which applies to state authorities, state administration bodies, local governments, legal entities with public authority and other legal and natural persons who have access to or are handling personal data and the implementing Government Decree published in the Official Gazette no. 58/10 require the implementation of security measures ensuring physical protection, protection of data, and protection of the information system. The information security measures under the Government Decree include:

(i) Measures of physical protection (establishment of administrative zone; development of a plan of physical protection; assessment of the effectiveness of physical protection measures; control of persons; data storage; physical protection of information systems.)

(ii) Data protection measures (mechanisms for data protection; access to the database; data storage requirements; encryption system for data protection)

(iii) Information system protection measures (setup and installation of servers, computers and networks; measures of protection against fire, humidity, cold and heat; application of cryptographic protection, etc.)

(iv) Risk management of information security (risk management; acceptance, reduction and risk avoidance; plan of activities).

FINANCIAL DATA

17

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 are no sector specific legal or regulatory requirements applicable to financial data that financial institutions need to be aware of while using cloud computing. Under the bank secrecy laws, persons who come into possession of data that represent bank secrecy, are obliged to use this information solely for the purpose for which they were obtained, and may not make them available to third parties, except as required by law. While the aforementioned banks secrecy regulation does not take into account cloud services specifically, it does not explicitly preclude financial institutions from outsourcing some of their functions and activities and it can be reasonably concluded that, subject to the cloud service provider maintaining the non-disclosure and secrecy obligation, financial institutions may deploy a cloud solution.

18

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

There are no such notification or approval requirements.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

There is no further guidance in this regard.

PENDING LEGISLATION

20

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

At this moment there is no pending legislation with potential impact on cloud computing.

RUSSIA

COUNSEL DETAILS:

Country: Russia

Attorney: Georgy Moshiashvili

Law Firm: PIERSTONE Moscow
c/o Kanashevsky & Partners Law Firm, LLC
12 Maliy Vlas'evsky Pereulok, 1
119002 Moscow
Russia

Website: www.pierstone.com

E-mail: georgy.moshiasvili@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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Federal Law On Personal Data No. 152-FZ, dated July 27, 2006 *(Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»)* (the "Privacy Act").

An English version of the Act is available at http://pd.rkn.gov.ru/authority/p146/p164/

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or the "DPA")? Summarize its powers.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) (Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications – Roskomnadzor, hereinafter referred to only as the "DPA").

Address: 109074 Moscow, Kitaygorodsky proezd 7, building 2

Website: http://eng.rkn.gov.ru/

Email: rsoc_in@rkn.gov.ru

Its competencies include:

(i) requesting from personal data operators the correction, blockage or destruction of inaccurate or unlawfully obtained personal data;

(ii) adopting measures for the suspension or termination of personal data processing if such processing is carried out in violation of law;

(iii) applying to court for the protection of rights of personal data subjects;

(iv) providing the Prosecutor's office and other law enforcement authorities with materials necessary for initiation of criminal proceedings against persons violating the rights of personal data subjects;

(v) bringing to administrative liability of persons breaching the requirements of the Privacy Act;

(vi) reviewing petitions and complaints of individuals and legal entities relating to personal data protection and adopting corresponding decisions within its powers;

(vii) maintaining a register of personal data operators.

The DPA is an independent central administrative body empowered to oversee compliance with the Privacy Act.

The DPA is entitled to perform supervision over the protection of personal data in accordance with the Privacy Act; decide on requests for protection of rights; deliver opinions with regards to the application of the Privacy Act; give consent with regards to the establishment of personal data filing systems; monitor the application of organizational and technical measures for the protection of personal data and propose improvement of such measures; put forward proposals and offer recommendations for the improvement in the protection of personal data; deliver an opinion as to whether a specific way of personal data processing puts rights and freedoms of individuals at risk; cooperate with authorities responsible for supervising the protection of personal data in other countries; cooperate with competent state authorities in the process of development of regulations relating to protection of personal data.

3

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

The provisions of the Privacy Act shall apply to the processing of personal data in the territory of Russia. The Privacy Act would thus in all likelihood also apply if a foreign data operator (controller) uses equipment located in the territory of Russia to process personal data there.

IMPORTANT DEFINITIONS

4

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 is defined as any information directly or indirectly pertaining to a specific or identifiable individual (personal data subject).

The law does not contain any provisions expressly stating or implying that encrypted personal data would no longer qualify as personal data. However if the personal data is initially encrypted by the data operator (cloud provider's customer) and is then transferred to the cloud provider (without encryption key or other means for deciphering the provided

data) it can be argued that such data does not qualify as personal (since it cannot be used for identification of any individual) and that for the given purposes the cloud provider does not act in the capacity of third party data processor

---

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

The Privacy Act divides personal data into 3 categories:

(i) personal data (general);

(ii) personal data of special category; and

(iii) biometric personal data.

The first category of personal data includes any personal data (other than the data included in the other two categories) and processing of such data is subjected to general requirements of the Privacy Act (e.g. personal data may be processed only subject to the consent of the personal data subject, personal data must be kept confidential by the persons carrying out its processing, etc.). The personal data of special category includes the data on individual's race, ethnicity, political views, religious views, philosophical views, health and private life. Biometric personal data includes data on physiological and biological features/ peculiarities of an individual. As a general rule, personal data of these two categories may be processed only subject to written consent of the relevant personal data subject. The Privacy Act stipulates the requirements for such written consent, which shall include, in particular, the following:

(viii) full name, address and ID details of the personal data subject,

(ix) full details of the personal data operator,

(x) the purpose of data processing,

(xi) the list of the personal data which is intended to be processed,

(xii) details of the person/entity to whom the data processing will be assigned by the data operator (if such assignment is intended),

(xiii) actions (operations) intended to be carried out by the data operator as well as the methods of data processing deployed by the operator,

(xiv) the timeframes within which the personal data shall be processed,

(xv) the signature of the personal data subject.

The aforementioned consent may be provided in an electronic form subject to compliance with the requirements of the Russian law on electronic signatures.

The Russian Government Decree No. 1119, dated November 1, 2012 establishes levels of protection (ranging from 1 to 4) in respect of personal data, where highest levels of protection are applied to personal data of special category and biometric personal data.

The Russian Government Decree No. 512, dated July 6, 2008 establishes requirements in respect of media on which biometric personal data is stored as well as in respect of technology deployed for the purpose of storing biometric personal data.

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

6

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

The Privacy Act does not use terms "data Controller" or "data processor". The equivalent of data controller (as defined by the EU Data Protection Directive) would be the "personal data operator" that is defined by the Privacy Act as ''a state authority, municipal authority, legal entity or individual who on its (his/her) own or jointly with other persons organizes and/or carries out the processing of personal data, as well as

defines the purpose of such processing, the content of personal data intended to be processed and the actions (operations) to be performed in connection with the personal data".

The personal data operator may assign the processing of personal data to a third party (such third party would be an equivalent of "data processor" as defined by the EU Data Protection Directive) subject to the consent of the personal data subject, under an agreement entered into by and between the personal data operator and such third party processor.

In the context of cloud computing, the cloud customer would be the personal data operator while the cloud provider would in most circumstances be the third party processor. The personal data operator (cloud customer) must obtain consent of the personal data subject prior to transferring the relevant data to a third party operator (cloud provider). The third party processor shall be under no obligation to obtain such consent from the personal data subject, however the third party processor shall comply with the general principles and rules of data processing established by the Privacy Act (e.g. the requirement to process the personal data for the pre-defined purposes, to store the personal data within the pre-defined time limits, to keep the personal data confidential, etc.) on par with the personal data operator. The personal data operator shall liable to the personal data subject while the third party processor shall liable to the personal data operator.

The key obligations of the personal data operator in the frame of processing personal data include the initiation of legal, organizational and technical measures for the protection of personal data from unlawful or unsanctioned access to such data, its unauthorized destruction, alteration, blocking, copying, transfer and other unlawful/unauthorized actions. Please refer to section 5.1 for more detailed description of such measures.

The key obligations of the third party processor shall be set forth in the agreement between the personal data operator and third party processor (refer to question 7 below).

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes, an agreement between a customer (personal data operator) and a cloud provider (third party processor) is required under the Privacy Act. Such agreement must specify the actions (operations) that the third party processor may perform with the personal data and the purposes of processing the personal data. Furthermore, the agreement should impose confidentiality obligations and the obligation to ensure the security of the data at the term for which it will be processed by the third party processor. The agreement should list specific security and organization measures (as per the non-exhaustive list provided by Section 19 of the Privacy Act) to be adopted by the third party processor for the protection of personal data. Refer to question 11 for the detailed description of such measures.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

The law does not provide for any restrictions in this regard. Therefore, provided that no such restrictions are stipulated by the agreement between a customer (personal data operator) and cloud provider (third party processor) and provided that the obligations similar to the ones undertaken by the third party processor under the agreement entered into with the personal data operator are imposed on sub-processors, the use of sub-processors shall be permissible.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

The Privacy Act does not distinguish between transfers to EU and non-EU countries. Transfer of personal data to countries that are the members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 108 ("Convention") is permissible subject to the general requirements of the Privacy Act. Briefly, in order for a Russian personal data operator to transfer

a Russian citizen's (personal data subject's) personal data to a third party processor from one of the countries being a party to the Convention, the Russian personal data operator (who has initially obtained the personal data subject's consent to the processing of his/her personal data) would need to notify the personal data subject of such transfer.

10

What are the requirements to transfer personal data to a non-EU country?

As noted above, the Privacy Act does not distinguish between transfers to EU and non-EU countries. In order to transfer personal data to a country that is not a party to the Convention or not included in the list of the countries ensuring adequate protection of personal data approved by the DPA, the personal data operator should first obtain from the relevant personal data subject a written consent to such transfer.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

Yes. Pursuant to the Privacy Act, the personal data operator shall implement technical and organizational measures to ensure the compliance with Russian law requirements regarding data protection, which include:

(i) appointment of a person responsible for the processing of personal data;

(ii) issuance of internal policy and local rules on processing of personal data for the prevention of violations of the Privacy Act requirements;

(iii) implementation of internal control and audit to ensure compliance of personal data processing with the requirements of the Privacy Act and implementation of personal data operator's internal policy on processing of personal data;

(iv) assessment of the harm that can be caused to the personal

data owners in case of breach of their rights and assessment of measures aimed at ensuring compliance with the personal data operator's obligations under Russian laws;

(v) familiarization of personal data operator's employees, directly involved in the personal data processing, with the Russian law requirements, internal policy and local rules on processing of personal data; providing trainings to personal data operator's employees;

(vi) taking all legal, organizational and technical measures for protection of personal data from unauthorized access, deletion, changing, blocking, coping, provision, distribution of as well as other unlawful actions in relation of personal data;

(vii) investigation of unauthorized access to personal data and taking necessary measures against such unauthorized access;

(viii) restoring the personal data which were modified or deleted as a result of unauthorized access to it;

(ix) providing rules for access to personal data and logging of all activities made with personal data in an information system;

(x) exercising control of protection measures implemented as well as provide for sufficient level of protection of personal data;

(xi) ensuring compliance with the following principles of processing of personal data: the processing of personal data shall be limited by specific purpose of the processing; the content and volume of processed personal data shall coordinate with the purpose of the processing; the processed personal data shall not be excessive and shall be commensurate to the purpose of the processing; the personal data shall be accurate and up to date; processor shall take all measures on specification or deleting of inaccurate or incomplete data; the personal data shall be stored no longer than it is necessary for the purpose of the personal data processing; the personal data shall be depersonalized or destroyed in case the purpose of the processing is reached;

(xii) performing only actions pursuant to the instructions of the operator and with the specific purpose of processing;

(xiii) ensuring the confidentiality and security of personal data in the course of their processing.

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

Yes. There are laws and regulations which are applicable to the financial and banking sectors and which contain certain rules that have certain relevance to cloud computing. *The Federal Law On Banks and Banking Activity No. 395-1 dated December 12, 1990 (as amended) (the "Banking Law")* stipulates that any information relating to banking secrecy may be transmitted by a bank to its parent credit institution or holding company located outside Russia only if the level of information protection (privacy) in such foreign jurisdictions is not lower than the level of information protection (privacy) prescribed by Russian laws (Art. 26 of the Banking Law). Therefore, by way of analogy, Russian banks and other credit institutions should be permitted to contract foreign cloud service providers only if the level of information protection (privacy) in the cloud provider's jurisdiction is not lower than the level of information protection (privacy) prescribed by Russian law.

Under *Russian Central Bank's Regulations on the Procedure of Creation, Maintenance and Database Storage on Electronic Media No. 397-P dated February 21, 2013 ("Regulation 397-P")* a credit institution shall store information about its assets, liabilities and all transactions in electronic databases for a period of at least five years, and such information must be accessible on each banking day. Regulation 397-P further requires that the electronic databases are up to date, the information contained in the electronic databases is recoverable, measures are taken to prevent damage, loss, malware infection, unauthorized modification and unauthorized access to the information contained in the electronic databases, and that backup copies of electronic databases are created. The Banking Law and Regulation 397-P do not contain any restrictions with regard to the storage of the credit institution's information abroad and/or the use of foreign cloud services for this purpose. Therefore storage of credit institutions' data in a cloud outside Russia is generally

permissible as long as the privacy, data retention, and security requirements described in this section are met.

In addition, the new Amendment to the Federal Law "On Information, Information Technology and Protection of Information" and Other RF Legislative Acts in Connection with Harmonization of Information Exchange via Information and Telecommunication Networks No. 97-FZ dated May 5, 2014 that entered in force in July 2014 and that introduced a mandatory 6 month retention requirement for electronic messages transmitted over the internet, is also likely to impact cloud computing providers if they qualify as "information distributors" for the purposes of this law . While this purportedly "anti-terrorist" legislative measure does not prohibit transmission of electronic messages outside of Russia, it imposes the retention obligation on the so-called "information distributors" to ensure that electronic messages remain available and accessible in Russia even after being transferred abroad. Currently, however, there is no relevant case law shedding light on the interpretation of this new law, including the practical implications of the definition of an "information distributor".

OTHER REQUIREMENTS

13

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. Thus, if the cloud provider would have to obtain consent of the relevant personal data subjects to processing their personal data for advertising purposes.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

No, the law does not explicitly provide for an audit right of the customer (personal data operator).

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

No, there are no prerequisites.

PUBLIC SECTOR

16

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

As a general rule, the requirements applicable to private sector would be likewise applicable to public sector. However, there are exceptions from this rule and the primary exception would be the processing of data relating to state secrets and other classified information. The processing of such data is regulated by special laws and specific protection requirements are applicable thereto.

Regulators in the public sector also impose additional requirements such as, in particular, the requirement that certain data of public authorities be stored only in databases (or state informational systems) that have met particular certification requirements.

In addition, state and municipal bodies may create their own databases of personal data and the operation of such databases is regulated by special laws. For example, under the Decree of the Russian Government

On Basic State Information Resources No 928 dated September 14, 2012, as amended, state bodies may include unique information about an individual or legal entity in the state information resources. Such information is intended for use in the interdepartmental cooperation in order to provide state and municipal services.

FINANCIAL DATA

17

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.

Russian law does not specifically regulate cloud services and/or the transfer of data in the context of cloud services. Similarly, there are no specific rules concerning the deployment of cloud services in financial and banking sectors. Nevertheless, the laws and regulations applicable to the financial and banking sectors contain certain rules that have some relevance to cloud computing. It is, in particular, the aforementioned Banking Law and Regulation 397-P which set forth certain security requirements for the handling and storage of certain data on electronic media (see response to question 5.2 above).

Russian law does neither expressly permit, nor expressly prohibit, banks and other financial institutions to use cloud services (whether provided by local or foreign cloud providers) or to store information in the databases situated outside of Russia. Therefore, the deployment of cloud solutions provided by foreign cloud service providers is generally permissible in the finance sector, subject to the cloud providers meeting the Russian law requirements and standards, particularly those pertaining to information security and data protection.

Storing and processing certain data of banks by cloud providers may trigger licensing and certification requirements (licensing of activities relating to protection of confidential information, as well encryption licenses, and certification of the information systems used for the storing and processing the data) which cannot be met by non-Russian entities. This may create a practical obstacle for a Russian bank to use a foreign cloud provider. At the same time, if a foreign cloud provider deploys,

in the frame of rendering cloud services, the information system and information protection means that provide the same (or higher) level of protection as the eligible Russian information systems and information protection means, it could be argued that such information systems and information protection means from technical perspective meet the general requirements of the applicable laws and regulations.

18

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

No notifications or approvals on the use of cloud computing are required under the Russian law. If cloud services provider is qualified as a "personal data operator" under the Personal Data Law it shall notify the DPA on its intention to perform processing of personal data prior to processing. Such notification is not required when personal data are processed in the cases provided by Personal Data Law (e.g. in accordance with labor law; for the fulfillment of the obligations of personal data owner under the contract; etc.). Operator shall provide the DPA with the documents and information on taken technical and organizational measures regarding data protection (see question 11 of this questionnaire) upon its request.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

There is no further guidance in this regard.

PENDING LEGISLATION

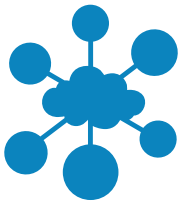
20

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

Pursuant to Federal Law No 242-FZ dated July 21, 2014 (as amended on 31.12.2014) the changes to the Privacy Act will come into force on September 1, 2015 and the purpose thereof is to establish further restrictions with regard to processing of personal data of Russian citizens. Under the amendment to the Privacy Act, upon the collection of any personal data of Russian nationals such data will have to be recorded, systematized, accumulated, stored, specified (updated or modified) and retrieved in the databases located in the Russian Federation. Pursuant to the new provisions of the Privacy Act, at the time of collection of personal data, inter alia over the Internet, the operator must ensure that the personal data of Russian individuals is recorded, systematized, accumulated, stored, specified (updated or modified) and retrieved in the databases located in the Russian Federation, except for the cases listed in clauses 2, 3, 4 and 8 of Article 6, section 1 of the Privacy Act (these exceptions include cases when personal data is processed in performance of an international treaty, for the implementation of judicial act, for the realization of powers of state authorities or for the achievement of professional objectives of journalists, mass media, etc.). Noncompliance with these requirements may result in blacklisting the violator and blocking access to the violator's information resource (i.e. in particular websites containing information processes and network addresses allowing the identification of the websites containing information processes in breach of the Privacy Act) on the basis of a court decision (prior to blocking the violator will be notified and given 1 business day from the receipt of the notification to remedy the violation). From the aforementioned retention provisions it is not clear whether the intention of the legislator is to prohibit entirely the transfer of the Russian individuals' personal data abroad or to simply ensure that such data is (simultaneously) stored in a database in Russia. The DPA representatives indicated on some occasions that they are inclined to the latter interpretations and that in their view the new law does not prohibit cross-border transfer of data, provided that the initial collection and storage of data is carried out on the territory of Russia. However, it yet remains to be seen what practice will eventually be adopted. Even

if the new retention obligation is interpreted less restrictively, i.e. as not preventing transfer of the personal data abroad, it will mean that personal data operators will not be able to export the personal data of Russian citizens outside the territory of the Russian Federation without simultaneously recording and saving such data in Russian databases. For foreign personal data operators this would effectively mean to store such data in databases (on servers) in the Russian Federation. Such requirement may present a significant limitation for foreign cloud providers.

SERBIA



COUNSEL DETAILS:

Country:	SERBIA
Attorney:	Marjan Poljak
Law Firm:	Karanovic & Nikolic
	Belgrade
	Serbia
Website:	www.karanovi-nikolic.com
E-mail:	marjan.poljak@karanovic-nikolic.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Law on Protection of Personal Data, published in the Official Gazette of the Republic of Serbia, nos. 97/2008, 104/2009, 68/2012 and 107/2012 (the "Privacy Act"). The Privacy Act is modelled upon the EU Privacy Directive; nevertheless, there are also certain substantial differences between the Privacy Act and the EU Data Protection Directive.

An English version of the Privacy Act is available at http://www.poverenik.rs/images/stories/dokumentacija-nova/zakon-o-zastiti-podataka-o-licnosti_en.pdf

2

Which authority oversees the data protection law (hereinafter referred to as the "data protection authority" or the "DPA")? Summarize its powers.

Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti ("Commissioner for Information of Public Importance and Protection of Personal Data", hereinafter referred to only as the "DPA").

Address: Bulevar kralja Aleksandra 15, 11000 Belgrade; www.poverenik.rs; email: office@poverenik.rs.

The DPA is an autonomous state authority empowered to monitor the implementation of the Privacy Act. It acts ex officio or upon complaint of an interested party and is empowered to conduct an inspection to establish whether the rules envisaged by the Privacy Act are respected. Should it establish any misconduct, the DPA is entitled, among other, to forbid temporarily the particular data processing and order deletion of the data collected without legal ground. In the case of the statutory rules' breach, it is also empowered to submit a request for the initiation of offence proceedings against an entity responsible for the respective breach. Furthermore, the DPA maintains the register of personal data processing operations (so-called Central Register) which is publicly available on-line. It is also authorized to approve a data transfer out of the country whenever such approval is required under the law.

3

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

The Privacy Act is generally applicable to the data processing carried out in the territory of the Republic of Serbia. This is applicable both in the case when a data controller is a locally established entity and in the case when a data controller is a foreign entity but the data processing is carried out on its behalf by a locally established data processor.

IMPORTANT DEFINITIONS

4

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?

Under the Privacy Act, personal data means "any information relating to a natural person, regardless of the form of its presentation or the medium used (paper, tape, film, electronic media etc.), regardless on whose order, on whose behalf or for whose account such information is stored, regardless of the date of its creation or the place of its storage, regardless of the way in which such information is learned (directly, by listening, watching etc., or indirectly, by accessing a document containing the information etc.) and regardless of any other characteristic of such information".

The Privacy Law does not prescribe the treatment of encrypted data. However, considering that only data based on which a natural person is identified or identifiable is regarded as personal data, it can be reasonably concluded that encrypted data without encryption key (i.e. without, presumably, a possibility of the data subjects' identification) should not be regarded as personal data.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

Yes. The Privacy Act prescribes stricter regime for so-called "particularly sensitive data". Under the law, particularly sensitive data includes "data relating to ethnicity, race, gender, language, religion, political party affiliation, trade union membership, health status, receipt of social support, victims of violence, criminal record and sexual life".

This data can be processed exclusively on the basis of a data subject's informed written consent which should contain the identification of the data, the processing's purpose and manner of its usage, save where the law does not allow the processing of such data even with the data subject's consent.

Exceptionally, some of this data (i.e. data regarding political party affiliation, health status and receipt of social support) can be processed without a data subject's consent, but only when such possibility is explicitly envisaged by law, e.g. a healthcare professional is allowed to disclose health related data of a patient to the members of the patient's family if such disclosure is necessary for the avoidance of health related risks by the patient's family members.

It should also be mentioned that, in the case of consent's withdrawal by a data subject who has previously provided such consent, a data controller is entitled to a remuneration of justified costs and damage suffered due to such withdrawal, unless otherwise stated in the consent form.

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

6

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

Under the Privacy Act, "data controller" is a natural person, legal entity or public authority responsible for the data processing and "data processor" is a natural person, legal entity or public authority to whom/which a data controller delegates certain processing-related duties under law or on the basis of a contract.

While the Privacy Act does not envisage any rules specifically governing cloud computing services, in light of the definitions of a data controller and data processor and, on the presumption that an entity providing cloud computing services processes the data solely on behalf and under instructions of a customer who owns the respective data, a cloud service provider should be regarded as a data processor and customer should be regarded as a data controller.

The key element of a relationship between a data controller and data processor (thus, between a customer and cloud service provider as well) is that a data controller has and retains control over the respective processing and is ultimately responsible for the same.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes, an agreement between a data controller and a data processor (thus, between a customer and cloud provider) is required, unless there is a statutory ground for the data processing by a data processor (i.e. cloud provider).

However, the Privacy Act prescribes no minimum content of this agreement. Under general principles of contract law and existing practice in the field of data protection, it should include the identification of both parties, types of the processed data, purpose and manner of processing and types of measures to be undertaken to ensure an adequate protection of the personal data processed.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Yes, the use of a sub-processor by a data processor (thus, by a cloud provider as well) is generally allowed.

There are no specific conditions or restrictions on the use of sub-processors other than those that may be prescribed by a data processing agreement entered into between a data controller and a data processor (which would typically require the data controller's approval of a particular sub-processor prior to its engagement by a data processor).

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

There are no specific requirements for the transfer of personal data to the EU, i.e. there is no need to obtain prior approval of the DPA. This is due to the fact that, pursuant to the Privacy Act, no approval of the DPA is required if personal data are transferred to any country which is a signatory of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter referred to as the "Convention"). The EU countries are parties to the Convention.

10

What are the requirements to transfer personal data to a non-EU country?

If a non-EU country is not a party to the Convention (e.g., the US), a prior approval of the DPA with the data transfer is necessary. The DPA evaluates, inter alia, whether the data protection legislation in force in the recipient country and the obligations undertaken by the data importer under the agreement with the data exporter provide sufficiently strong protection of the data which are to be transferred. It also assess whether the general data protection requirements (such as the legitimacy of the purpose for which the data are to be transferred and whether the processing/transfer us reasonably necessary for achieving the purpose) are met. The DPA is known to be very strict when it comes to the grant of approvals for data transfers to such third countries.

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

The Privacy Act does not prescribe any particular security requirements to be fulfilled by data processors (or data controllers). It only provides for a general requirement that: (i) personal data must be adequately protected from abuse, destruction, loss, unauthorized alterations or access, and that (ii) both data controllers and data processors implement all necessary technical, personnel and organizational measures to protect data from loss, damage, unauthorized access, modification, publication and any other abuse, and that the data are kept confidential by all persons engaged in the data processing.

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

No, there are no such other laws or regulations.

OTHER REQUIREMENTS

13

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

No. All personal data can be used only for legitimate purposes previously approved by the data subjects and their use for marketing purposes must be subject to prior written approval of the data subjects as well.

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

The Privacy Act does not prescribe any particular rules with respect to audit. However, relevant audit rights may be included into a data processing agreement by its parties, including the manner of performing such audit, i.e. whether it would be performed by a data controller itself and/or by an independent auditor (including the one selected by a data processor).

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

No, there are no specific prerequisites in this regard, except if a customer is planning to transfer personal data to clouds in the countries which are not members of the Convention. In such case, prior data transfer approval of the DPA is a precondition for the commencement of a particular cloud provider's engagement.

PUBLIC SECTOR

16

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

No, there are no different data protection requirements generally applicable in only one of these sectors but not the other.

FINANCIAL DATA

17

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 Decision on Minimum Standards of Managing Information System of Financial Institution (Official Gazette of the Republic of Serbia, nos. 23/2013 and 113/2013) applies to the processing of financial data. Pursuant to the Decision, a financial institution intending to outsource some of its activities is required to notify the National Bank of Serbia at least 30 days prior to conclusion of an agreement with a third-party service provider. Prior to making a decision on each outsourcing and/or on the change of the service provider, the financial institution is required (among other things) to determine whether the legislation of the country in which the service provider operates enable the National Bank of Serbia to smoothly perform on-site control of operations in the segment relating to the performance of the outsourced activities (or related activities) on the premises of the service provider. The financial institution is required to enable the National Bank of Serbia to perform such audit upon its request. In addition, the financial institution is required to ensure that the service provider grants to an external auditor engaged by the financial institution and the National Bank of Serbia a timely and unlimited access to the documentation and data relating to the outsourced activities.

18

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

Yes. Financial institutions intending to outsource some of their activities are required to notify the National Bank of Serbia at least 30 days prior to conclusion of an agreement with a third-party service provider. Please see the response to question 17 above.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

No, there is no such guidance.

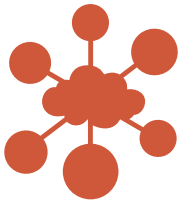
PENDING LEGISLATION

20

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

The current Privacy Act is expected to be replaced, in the foreseeable future, by a new Law on the Protection of Personal Data. While the draft of the new law envisages a number of changes to the current Privacy Act (for example, it prescribes the mandatory content of a data processing agreement or provides for more detailed rules governing the procedure for issuance of a data transfer approval), it does not introduce any rules explicitly governing cloud computing.

UKRAINE



COUNSEL DETAILS:

Country: Ukraine
Attorney: Iryna V. Kalyta
Law Firm: Ernst & Young
19a Khreshchatyk street
Kyiv
Ukraine
Website: http://www.ey.com/ua
E-mail: Iryna.Kalyta@ua.ey.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.

INTRODUCTION

1

In general, what is the statutory basis for the protection of personal data (hereinafter referred to as the "Privacy Act")?

Law of Ukraine "On Personal Data Protection" No. 2297-VI dated 1 June 2010, as amended and supplemented (the "Privacy Act"). Overall, the Privacy Act is based on the EU data privacy legislation, namely the EU Data Protection Directive. Nevertheless, there are also certain substantial differences between the Privacy Act and the EU Data Protection Directive (some of these related to flawed adaptation of the Directive's provisions).

There are no specific laws and regulations in Ukraine governing processing of data using cloud computing technologies, so general Ukrainian data protection rules apply.

2

Which authority oversees the data protection law

Уповноважений Верховної Ради України з прав людини (the Ukrainian Parliament Commissioner for Human Rights, hereinafter referred to as the "data protection authority" or the "DPA").

Address: 21/8 Instytutska St., Kyiv 01008, Ukraine; http://www.ombudsman.gov.ua/; email: hotline@ombudsman.gov.ua

The DPA is entitled, inter alia, to issue personal secondary regulations regarding data processing where provided for by the law, to monitor compliance with the personal data protection requirements, and to carry out on-site and remote, scheduled and unscheduled inspections of data controllers and data processors.

The DPA is authorized to access any premises where personal data is processed, as well as to receive from data controllers and data processors any information (including classified information) required for purposes of control of compliance with personal data protection requirements. Upon such inspections the DPA is authorized to issue binding orders to rectify discovered violations of personal data protection requirements, as well as to impose administrative sanctions on data controllers' and data processors' officials subject (although they have to be further confirmed by the court).

Also, the DPA addresses complaints, requests and inquiries of individuals and legal entities, and issues clarifications and recommendations concerning compliance with the personal data protection regulations.

3

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

The scope of application of the Privacy Act in terms of territoriality is not explicitly defined.

Generally, all data controllers and data processors having presence in Ukraine and/or performing within Ukraine any of the operations with personal data that qualify as "personal data processing" under

the Privacy Act (i.e., collect, register, accumulate, store, adapt, alter, retrieve, use and disseminate (distribute, sale, transfer), depersonalize, or destroy personal data), must ensure compliance with Ukrainian data privacy regulations.

It is unclear to which extent Ukrainian data protection regulations should apply to data controllers and data (sub)processors (including cloud service providers) not having presence in Ukraine where they process personal data received from Ukraine outside the territory of Ukraine.

There is a general statement in the Privacy Act that a third party may not be granted access to personal data if it refuses to be bound by the obligation to be in line with the Privacy Act, or if it is not capable of doing so.

The Privacy Act also establishes certain requirements with respect to transfer of personal data to "foreign persons". Generally, these requirements impose responsibility on data controllers and processors for ensuring that the personal data transferred is protected adequately, i.e., in line with Ukrainian rules. Thus, a data controller processing personal data within the territory of Ukraine and intending to transfer this data to a processor (including to a cloud provider) for its processing outside the territory of Ukraine, should consider provisions of applicable Ukrainian regulations, as well as recommendations of the Ukrainian DPA, particularly when drafting and negotiating the relevant contractual clauses.

IMPORTANT DEFINITIONS

4

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?

Under the Privacy Act, "personal data" means "a piece of information or aggregated information about an identified or specifically identifiable individual".

There are no explicit indications on whether encrypted personal data could or could not be considered personal data in case the encryption key is not available to the person processing such data.

Based on general provisions of the Privacy Act, if data is depersonalized and the relevant individual ceases to be identified or identifiable, such data is not considered "personal data" and, consequently, is not subject to the protection. Yet, no official recommendations or guidelines have been issued by the DPA in this regard so far.

5

Does the Privacy Act differentiate between different categories of data to which it affords a level of protection that goes beyond the normal requirements for personal data outlined in this questionnaire; e.g. sensitive data, such as health information? Please list the most relevant differences.

Yes. The Privacy Act provides for additional requirements regarding processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties and trade-unions, criminal records, as well as data concerning health or sex life, biometric or genetic data. Additional requirements would apply if: (i) personal data includes any of the data categories mentioned above, or (ii) the controller processes personal data of general nature in relation to data subjects who can be distinguished into a separate category based on the categories of data above (e.g., personal data of general nature is processed only with respect to data subjects who have criminal records).

Personal data belonging to this category may only be processed if one of the conditions prescribed by the Privacy Act is met:

(i) the data subject has given explicit consent to the processing;

(ii) processing is necessary in light of specific employment-related rights and obligations of the controller, subject to protection requirements;

(iii) processing is necessary to protect vital interests of the data subject or of another person where the data subject is restricted in his/her legal capacity or is legally incapable;

(iv) processing is performed by a religious organization, political party or a trade union in connection with its activities, subject to certain restrictions;

(v) processing is required to justify, protect or satisfy a legal claim;

(vi) processing is needed for healthcare purposes (conditions apply);

(vii) processing of data relates to criminal court verdicts or is performed as part of combatting terrorism;

(viii) processing relates to data which is manifestly made public by the data subject.

There is also an additional requirement for data controller to notify the DPA about processing of sensitive personal data within 30 days of the beginning of the processing. The procedure of such notification is adopted by the DPA[1]. This requirement applies to data which, when processed, is likely to present specific risks to the rights and freedoms of data subjects. In addition to the types of data indicated above, this category covers data revealing national origin, membership in religious and philosophical organizations, administrative liability records, measures taken in course of criminal investigation, facts of violence having been committed towards a person, person's location and movements.

For purposes of transfer and in regard to other obligations of data controller and data processor, sensitive categories of personal data are treated equally as other categories of personal data.

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

6

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

Ukrainian regulations do not specifically address matters related to cloud computing. Under general rules of the Ukrainian Privacy Act, the data controller is defined as "a natural or legal person that determines the purpose of the processing of personal data, the composition of such data and the procedure for its processing", whereas the data processor

is “a natural or legal person authorized by a data controller to process personal data on behalf of such data controller”[2].

Based on these definitions, in an arrangement where the cloud provider is engaged by a customer which collects/receives data pertaining to individuals, the cloud provider would likely be a data processor while the customer would be a data controller. However, there may be situations where the cloud provider may be regarded as data controller (if the data is processed for the cloud provider’s purposes) or as a third party (particularly, if the customer is itself a data processor). Distribution of roles in the situation where cloud computing service is provided through a chain of intermediaries is uncertain.

Generally, the key obligation of both data controller and data processor is to ensure that personal data is protected against accidental loss and unauthorized processing, including unlawful destruction and unlawful access to personal data. The responsibility of ensuring the required personal data protection regime in case of further transfer of such data rests with a person transferring the data.

Apart from the above, data controller solely bears responsibility for notification of data subject of transfer of personal data to the third party (if provided by terms of data subject’s consent or unless otherwise is provided by the law), as well as of alteration, deletion, destruction and restriction of access to personal data. Furthermore, data controller should notify the DPA about processing sensitive personal data that may present risks for data subjects’ rights and interests.

Data subjects have certain rights (e.g., the right to access to its data, to know where and by whom the data are processed and transferred to, the right to demand changing or deletion of the data etc.). In some cases data subjects could make recourse either to controller or to the

1 Procedure for Notification of the Ukrainian Parliament Commissioner for Human Rights on Processing of Personal Data Presenting High Risk for Rights and Freedoms of Data Subjects, approved by Order of Ukrainian Parliament Commissioner for Human Rights No.1/02-14 dated 8 January 2014.
2 Confusingly, the Privacy Act translates “data controller” as “data holder”, and “data processor” roughly as “data controller”. As these are clearly translation defects, we are using the internationally accepted terminology.

processor (or to both). In many cases it is not clear to whom the data subject should apply to ensure protection of his or her rights.

Further, only state or municipal authorities and state or municipal enterprises that belong to the domain of the former may act as processors of personal data if state or municipal authorities are controllers of such data.

7

Does the Privacy Act require an agreement between a customer and a cloud provider? Describe its minimum content.

Yes, assuming that the customer is a data controller and the cloud provider is a data processor.

The Privacy Act requires an agreement in writing between the data controller and the data processor. The agreement should specify the scope and the purpose of personal data processing, as well as generally required terms, i.e., subject matter, price and duration. More details are generally recommended in order to enable the controller to abide by its obligations set out by law. For specific conditions which may be required for agreements in certain cases of cross-border transfers of personal data, refer to questions 9 and 10

Where the cloud services are provided through a chain of intermediaries, there is ambiguity as to the distribution of roles among parties to such a setup. As a result, there is no clarity regarding the parties between which data processing agreements are required.

8

Is the use of sub-processors by the cloud provider permissible? If so, are there any specific conditions or restrictions on the use of sub-processors?

Technically, the use of sub-processors by the data processor is not prohibited by the Privacy Act, but is not explicitly addressed either. However, under the Privacy Act, any onward transfers of personal data by a data processor are at risk of being considered transfers to a third party and therefore require prior consent of data subject. Also, the data controller remains responsible for notifying the data subject about any

onward transfer of personal data to any third parties (if provided by terms of data subject's consent or unless otherwise provided by the law), which should include transfer of data to sub-processors.

Prior to the transfer of personal data to the sub-processor, the processor must take measures to ensure that the protection requirements of the Privacy Act are met by such a sub-processor.

INTERNATIONAL DATA TRANSFERS

9

What are the requirements to transfer personal data to the EU?

The Privacy Act allows cross-border transfer of personal data only as long as the country to which the personal data is transferred ensures an adequate level of protection. All EU/EEA member states are considered offering such level of protection. Thus, generally, the following key elements should be considered when transferring personal data to the EU/EEA member states:

(i) the processing itself and grounds for such processing must comply with Ukrainian data protection regulations;

(ii) unambiguous and specific consent shall be received from data subject for the proposed transfer[3];

(iii) an agreement in writing should be concluded between data controller and data processor specifying at least purpose and scope of personal data processing, as well as, arguably, subject matter, price and duration.

3 There is no established administrative practice on this matter. Whereas the Privacy Act may be reasonably interpreted as not to require a specific data subject's consent for transfer of personal data to an EU/EEA member state, the DPA's approach is rather conservative and the DPA is likely to insist on a specific consent given by the data subject.

10

hat are the requirements to transfer personal data to a non-EU country?

In addition to EU/EEA member states, states signatory to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the "Convention") are considered to ensure an adequate level of personal data protection by virtue of the Privacy Act. Therefore, transferring personal data to such countries is to be performed on the same conditions as transfer of personal data to the EU/EEA member states (see question 9).

Regarding transferring personal data outside the territory of Ukraine to countries that are neither EU/EEA member states nor signatories to the Convention (e.g., the USA), the provisions of the Privacy Act are rather ambiguous. Ukrainian privacy regulations do not explicitly state what specific requirements should be met in such cases.

The DPA has issued guidance stating that in case of transfer of personal data to countries that are neither EU/EEA member states nor signatories to the Convention, the agreement between data controller and data processor should contain provisions which ensure fundamental rights of the data subject, namely the right to access his/her personal data; the right to be acquainted with the location of his/her personal data, the right to submit a reasoned demand to the data controller and data processor for change or destruction of his/her personal data, and the right to submit claims regarding processing of his/her personal data to respective state authorities or courts. In this regard, the DPA recommends using the Agreement on Personal Data Transfer that was developed by American Chamber of Commerce and overall reflects the principles of standard contractual clauses (controller-processor) for the transfer of personal data to third countries approved by the European Commission[4].

Also, similarly to the transfer of personal data to the EU/EEA member states, there should be a legitimate basis for processing of personal data in accordance with the Privacy Act, and it would likely be required that the data subject gives prior consent for the specific cross-border transfer.

4 Available at http://www.chamber.ua/files/documents/updoc/32/Agreement_PD_transfer_cont_proc_Chamber_logo.pdf

SECURITY

11

Does the Privacy Act impose any security requirements (technical and organizational measures) for cloud providers (or data processors, generally)? Please list the key requirements.

While imposing on data controllers and data processors a general obligation to protect personal data from accidental loss or destruction and from unauthorized processing, including unlawful destruction and access, the Privacy Act does not specify any technical or organizational security measures that must be taken by data processors (including cloud providers).

However, the Standard Procedure for Personal Data Processing[5] that was adopted in accordance with and on the basis of the Privacy Act stipulates that the data controller and the data processor should take measures aimed at protection of personal data during all processing stages, including technical and organizational measures. Furthermore, they should at their own discretion determine the list and the scope of measures aimed at ensuring the security of personal data.

Under the Standard Procedure for Personal Data Processing, organizational measures which must be undertaken by data controllers/ data processors include, in particular:

(i) establishing a procedure for access of data controller's / data processor's employees to personal data;

(ii) establishing a procedure for tracking of operations related to processing of personal data and access thereto;

(iii) development of an action plan in case of unauthorized access to personal data, damage of technical equipment and emergency situations;

(iv) arranging periodic trainings for employees who operate with personal data.

5 Standard Procedure for Personal Data Processing, approved by Order of the Ukrainian Parliament Commissioner for Human Rights No.1/02-14 dated 8 January 2014.

12

Are there any other laws / regulations that impose specific security requirements for cloud providers?

Yes, laws and regulations on information protection in Ukraine comprise a number of security requirements that should be met where certain types of information are processed. For example, information circulating within all types of state institutions' information systems, as well as any information that must be protected according to the law[6], requires protection with the comprehensive information protection system. This, inter alia, means that all components of information systems processing such information should meet numerous technical, cryptographic and organizational requirements and must be either certified or examined with respect to compliance with these requirements by the authorized bodies. These requirements are notoriously burdensome and outdated. Nevertheless, despite the fact that both private and public entities may be audited in this regard by the relevant controlling authorities, in practice only state and municipal institutions maintain compliance with the above requirements.

OTHER REQUIREMENTS

13

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

No, unless the data subject specifically agrees to this when providing his/her consent for the data processing. If the cloud provider mines the customer data for its own purposes and not as instructed by the customer acting as data controller, the cloud provider will likely be regarded as a data controller with respect to such customer data. Thus, the cloud provider would itself be responsible for compliance with the data protections laws, including with respect to obtaining proper consent for data processing.

6 This category includes, particularly, state secrets, "official information" (lower-level state-owned classified data), non-state secrets (e.g., bank secrets, medical secrets), and confidential information. These types of information (especially confidential information) may potentially include personal data..

14

Does the customer have the right to audit the cloud provider? Can the parties instead agree to an audit by an independent auditor selected by the cloud provider?

Neither the Privacy Act nor the DPA's regulations on personal data protection explicitly entitle the data controller (customer) to audit the data processor (cloud provider) ipso jure. However, relevant audit rights may be included into a data processing agreement by its parties.

15

Are there any prerequisites for a customer to use cloud services (such as notification or approval from the data protection authority)?

No, the Privacy Act does not require any notifications or approvals for the use of cloud services from the DPA. In the absence of any specific regulations, the use of cloud services in Ukraine is subject to general rules regarding processing of personal data and, particularly, the transfer of such data to any data processor, regardless of whether the latter is a cloud provider.

PUBLIC SECTOR

16

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

Yes. Only state or municipal authorities and state or municipal enterprises that belong to the domain of the former may act as processors of personal data if state or municipal authorities are controllers of such data. Thus, the use of cloud computing by public bodies is to a large extent precluded by the above restriction, unless the cloud provider belongs to the domain of the respective state or municipal authority.

There are also restrictions on connecting the systems that process some types of state-held information to the Internet.

FINANCIAL DATA

17

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.

Information security and, consequently, the use of any IT services in banks are subject to various additional restrictions and requirements specified in vast amount of statutory acts. In particular, great amount of financial information is regarded as classified information under Ukrainian regulations and, therefore, general restrictions of the protection of information are also applicable to such financial information. (For an outline of general restrictions and requirements regarding information security, refer to question 12). Also, any personal data contained in financial data is covered by general regulations on personal data protection.

Apart from this, there are some specific statutory provisions regulating banks' IT activity which can also impede the use of cloud computing. In particular, any transfers of data that constitute bank secret may be made via encrypted channels only. According to Regulation on Arrangement of Operations in the Banks of Ukraine, all information on operations must be processed and stored on servers and other computing equipment physically located within the territory of Ukraine and in the premises that meet specific technical requirements[7]. However, none of the legislative acts actually provide for the definition of "information on operations", thus the actual use of cloud computing in financial sector is impeded due to this uncertainty.

Furthermore, certain operations with information can only be performed by banks with the use of software provided by Ukraine's central bank – the National Bank of Ukraine (e.g., completing of documents in the system of electronic payments).

Also, all banks must have information security management systems implemented in accordance with the standards adopted by the National Bank of Ukraine (based on ISO/IES 27001:2005 and ISO/IES 27002:2005).

7 Regulation on Arrangement of Operations in Banks of Ukraine, approved by Resolution of the National Bank of Ukraine No. 254 dated 18 June 2003.

18

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

No additional notifications to or approvals from the National Bank of Ukraine or any other regulatory authority are specifically required for use of cloud computing by financial institutions.

GUIDANCE NOTES AND RECOMMENDATIONS

19

Is there any local guidance on cloud computing issued by the data protection authority or any other relevant authority / regulator?

No, there is no such guidance. However, the following general recommendations of the DPA on various personal data protection matters may be relevant to cloud providers:

(i) Letter of the State Service of Ukraine on Personal Data Protection Concerning Storage of Documentation (Databases) Outside the Territory of Ukraine, No. 10/2306-13, dated 3 September 2013;

(ii) Clarifications to the Standard Procedure for Personal Data Processing, issued by the Ukrainian Parliament Commissioner for Human Rights on 8 January 2014;

(iii) Clarification to the Procedure for Notification of the Ukrainian Parliament Commissioner for Human Rights on Processing of Personal Data Presenting High Risk for Rights and Freedoms of Data Subjects, issued by the Ukrainian Parliament Commissioner for Human Rights on 8 January 2014.

8 The State Service of Ukraine on Personal Data Protection had been the authority in charge for personal data protection matters until its competences were transferred to the Ukrainian Parliament Commissioner for Human Rights starting 1 January 2014..

PENDING LEGISLATION

20

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

Currently, there are no draft laws or regulations addressing the use of cloud computing in Ukraine. However, due to the recent political changes in Ukrainian parliament and government, the legislative process with respect to a broad variety of matters is currently in its active phase. It is nevertheless hard to foresee whether the regulations on personal data protection and/or cloud computing specifically will be amended and/or developed in the nearest future.