CLOUD COMPUTING IN SLOVENIA

3rd Edition

REGULATORY FRAMEWORK

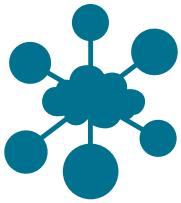


TABLE OF **CONTENT**

FOREWORD

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

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

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 **Nastja Rovšek Srše** of the law firm **Kanalec, Dren, Rovšek Srše in Ljubljana, Slovenia.**

The article Think Cloud Compliance – Achieving Trust and Compliance in the Cloud was written by Rich Sauer, Corporate Vice President and Deputy General Counsel, Microsoft Corporation.

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

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

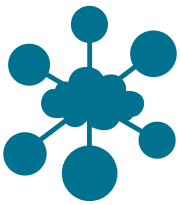
HOW TO USE THIS PUBLICATION

This publication consists of four parts.

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

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

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



TERMS USED IN THE QUESTIONNAIRE SECTIONS

Cloud Opinion	Opinion 05/2012 on cloud computing released by the EU Article 29 Working Party (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf)
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)
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 Data Protection Regulations	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1481555366159&uri=CELEX:32016R0679)
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 Privacy Shield Framework	European Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 65/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU- U.S. Privacy Shield (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL)

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) declared invalid by the Judgement of the Court (Grand Chamber) of 6 October 2015 - Maximilian Schrems v Data Protection Commissioner (case C-362/14).
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

ACHIEVING TRUST AND COMPLIANCE IN THE CLOUD

International In-house Counsel Journal

Vol. 9, No. 36, Summer 2016, 1

Rich Sauer,

Corporate Vice President

and Deputy General Counsel,

Microsoft Corporation

The accelerating shift from traditional on-premises information technology ("IT") systems to cloud computing presents in-house counsel with a veritable obstacle course of compliance challenges and regulatory pitfalls. Virtually every industry today faces an expanding set of data security demands, while different countries often have their own unique privacy and data protection requirements. Even global regulatory landscapes can change with the stroke of a pen, as with the recent invalidation of the long-standing Safe Harbor data transfer arrangement between the EU and United States. Today's in-house counsel must master all of these requirements, explain them to their boards, and verify that their organization complies with them.

The cloud is all around us in modern enterprise computing. Here is a brief list of some common examples:

- Cloud email and productivity services: Microsoft Office 365, G Suite
- Full-fledged cloud-based business applications: Salesforce.com for Customer Relationship Management (CRM), Workday for Human Resources Management and ERP
- Cloud-based virtual servers that can be launched in minutes and operated on a pay-as-you-go basis for any business or web application: Amazon Web Services (AWS), Microsoft Azure, IBM Softlayer
- Cloud-based machine intelligence: Microsoft Azure, IBM Watson
- Cloud-based data storage that expands or contracts flexibly with requirements: Box, Dropbox

For a technology vendor, keeping a broad portfolio of feature-rich cloud services in compliance with an ever-changing regulatory landscape

is–by definition–a never-ending challenge. At Microsoft, our own lawyers engage daily with our cloud engineering teams to help them understand and implement the requirements of this complex and evolving regulatory universe. This article will discuss Microsoft's experience working to meet the exacting legal and compliance requirements of our customers around the world.

By reviewing several particularly thorny regulatory and compliance issues that Microsoft has grappled with, this article also discusses several technical developments that in-house counsel need to understand as they evaluate cloud services. Our fundamental message is simple: the economic and strategic advantages of cloud computing make it impossible to ignore, but the transfer of responsibility over sensitive data and applications from customers to cloud providers requires the formation of a new framework for establishing and maintaining trust between these contracting parties.

EVERY BUSINESS WILL BE A DIGITAL BUSINESS: WHY THE CLOUD IS SURGING

After decades of unceasing progress in computers and software, we are all familiar with the tech industry's tendency to overhype each new innovation. Every press release seems to herald a new era, every product promises to change the world. But after a few months or quarters of excitement, the new technologies launched with great fanfare often turn out to be only incremental improvements, not revolutionary breakthroughs.

We all recognize that pattern. However, this innovation truly is different. The cloud really is a revolution, and it really will change the world. In fact, it is already doing so.

To understand why the cloud is different, we can divide the past half century of computing into four epochs. The first was the epoch of the mainframe, behemoths so big and expensive they could only function inside dedicated buildings owned by giant corporations. This epoch was dominated by IBM.

The four epochs of business computing

Epoch 1
Mainframe

Epoch 2
PCs

Epoch 3
Internet

Epoch 4
Cloud

“Although we think of the Internet as the foundation of our modern high tech world, in reality the Internet epoch was only a brief interlude.”

The second epoch was that of the PC, launched in the early 1980s by Apple, Microsoft and Intel. These inexpensive desktop computers were first marketed to hobbyists and consumers, but soon swept the corporate world, penetrating into even the smallest organizations. By the 1990s, evolved versions of the PC known as servers also came to stand alongside mainframes in corporate data centers. But these servers still lacked the power to handle the most important “mission-critical” tasks.

By the latter half of the 1990s, the third epoch of computing emerged with the connection of hundreds of millions of client and server PCs into a vast global network. Known as the Internet, this network made possible countless new applications built on the reality that any individual could now instantly communicate with any other individual or access the information and processing power of any other computer on the planet.

Although we think of the Internet as the foundation of our modern high tech world, in reality the Internet epoch was only a brief interlude. Over the past few years, it silently mutated into something new, which we now call the cloud. This new epoch is a combination of the previous epochs, but innovations in software and hardware make the cloud almost unimaginably more powerful than previous computing paradigms. After the extreme decentralization of IT brought about by the PC and the Internet, the “cloud” is all about the recentralization of the world’s data and computing power into a relative handful of “hyper-scale” data centers. A single one of these facilities may house tens or even hundreds of thousands of PC-like servers packed into energy-efficient, massively interconnected racks spread out over the space of a football field or more.

$200 billion+

Global spending on commercial cloud services this year

The growth of the cloud in the early 21st century is strikingly similar to the rise of the electrical grid in the early 20th century. In 1905, when every factory needed to generate its own electricity on site, the United States counted 50,000 separate electrical power plants, typically using proprietary and incompatible standards. But within a few decades, even as the nation's economy and electric power needs grew tremendously, 95% of those local plants had disappeared, replaced by a vast national grid where almost all power was generated in a few giant facilities.[1]

Today we are witnessing a similar transition in the organization of what we may call "information energy." Within the next 10 years, the majority of business applications and virtually all consumer applications will be served from perhaps a few hundred of these huge cloud data centers, located in all of the world's major geographies. Owing to its tremendous economies of scale, on-demand usage model, and pay-only-for-what-you-use billing, the cloud will progressively make inroads into the IT infrastructure of nearly all enterprises.

500% faster

Cloud applications growth compared to traditional on-premises IT

How confident should we be about rosy forecasts for the cloud's future? As the father of quantum mechanics Niels Bohr once said, "Prediction is very difficult, especially about the future." However, there is a clear and strong consensus among analysts that cloud growth forecasts are grounded in reality. Analyst firm Gartner estimates that global spending on commercial cloud services will pass $200 billion this year.[2] Investment bank Oppenheimer recently advised its Wall Street clients that the share of global compute capacity operated by the major cloud providers will likely approach 65% in the next five years.[3] Network manufacturer Cisco, whose equipment transports a large share of the world's Internet traffic, estimates that cloud applications are growing 500% faster than traditional on-premises IT.[4]

1 "Cloud Surfing: A New Way to Think About Risk, Innovation, Scale, and Success," Tom Koulopoulos and Jim Champy, 2012.
2 "Global public cloud market expected to hit $204B in 2016," ComputerWorld, January 26, 2016 (http://www.computerworld.com/article/3026396/cloud-computing/global-public-cloud-market-expected-to-hit-204b-in-2016.html).
3 "Cloud Surfing: A New Way to Think About Risk, Innovation, Scale, and Success," Tom Koulopoulos and Jim Champy, 2012.
4 "Cloud Surfing: A New Way to Think About Risk, Innovation, Scale, and Success," Tom Koulopoulos and Jim Champy, 2012.

THE CLOUD IS TRANSFORMING THE COMPLIANCE LANDSCAPE

"…on-premises data centers are now being "cloudified" by an additional layer of automation and management software that transforms these on-premises facilities into…"private clouds."

No one is predicting the complete disappearance of traditional in-house IT. On-premises IT systems will remain a vital part of enterprise computing for many years to come, especially to handle particularly sensitive data or mission-critical workloads. However, the cloud is disrupting even on-premises workloads. In the past decade, most enterprise IT organizations have embraced the software technique known as virtualization, which allows each individual hardware server to be shared by multiple "virtual" servers, thus yielding significant cost savings due to more efficient utilization of expensive capital equipment. Having first been virtualized, traditional on-premises data centers are now being "cloudified" by an additional layer of automation and management software that transforms these on-premises facilities into what industry analysts call "private clouds."

Large organizations are increasingly using private clouds to distribute internally generated "information energy" to their multiple business units, hoping to capture some of the flexible resource allocation and economies of scale offered by public cloud services. For instance, Microsoft offers a private cloud version of its public Azure cloud service known as Azure Stack. For customers using this software, servers and other computing assets in on-premises data centers are managed in much the same way that Microsoft operates the hardware and software in its public cloud data centers. Indeed, at the click of a mouse, customers can shift applications seamlessly

from their private Azure cloud to Microsoft's public cloud. In many cases, such readily hybridized private clouds will serve as a way station to the public cloud.

It is also true, of course, that the rise of the cloud does not mean distributed computing power will go away. On the contrary, the innumerable cloud applications and the oceans of information (including video, images, text, and quantitative data) that live in hyper-scale cloud

"…cloud computing introduces a level of legal complexity that requires a fundamentally new way of working and thinking by in-house counsel."

data centers will be continuously connected via the Internet to many billions of end devices. The latter will include smart phones, tablets, PCs, and—last but not least—the oncoming tidal wave of "Internet of Things" sensors. But increasingly, the applications and services that make these devices useful will be powered by the cloud.

The economic and strategic benefits of cloud computing are too large for even the most risk-conscious organizations to forego. Indeed, because the cloud will increasingly be a strategic asset for innovation and productivity for companies across the economy, almost every business in the future will be a digital business.

But by shifting the permanent residence of data and applications to data centers owned by third parties that may be located in other countries or even on other continents, cloud computing introduces a level of legal complexity that requires a fundamentally new way of working and thinking by in-house counsel.

This article turns to these issues in the following sections. It begins with concrete examples of cloud computing and the compliance challenges it raises. It then reviews the types of cloud compliance issues that Microsoft has confronted on behalf of its customers. Finally, it comments briefly on how a large cloud provider like Microsoft conceives of compliance as an actual service that must be built to the same rigorous specifications as all our other products.

HOW THE CLOUD RAISES NEW COMPLIANCE CHALLENGES: THE EXAMPLE OF LAW ENFORCEMENT

When machines recognize faces and understand speech, we must pay extra attention to privacy.

In the past five years, researchers in universities and corporate R&D labs such as those of Microsoft, Facebook and Google have made dramatic progress in machine learning. Researchers now have a very good idea of how to build software that understands human speech and recognizes human faces. This field is moving more quickly than many people in the legal community may realize. In the past two years, such software has moved out of the research labs and into production in large consumer-facing applications such as Microsoft's Cortana digital assistant, Facebook's photo face tagging, and Google Photos. Now, machine learning is poised to break out of the consumer market and into the enterprise. Automated understanding of text, speech, images and video will very quickly become a standard feature of enterprise IT applications, from the most routine to the most strategic.

Training the models that power machine learning requires immense amounts of data and compute power. As a result, most production-caliber machine learning applications will have to reside in the cloud.

Question: When software in the cloud can understand the words and recognize the faces of vast numbers of individual users, what measures must enterprises and their cloud providers take to ensure compliance with legal mandates for privacy and the protection of personally identifiable information?

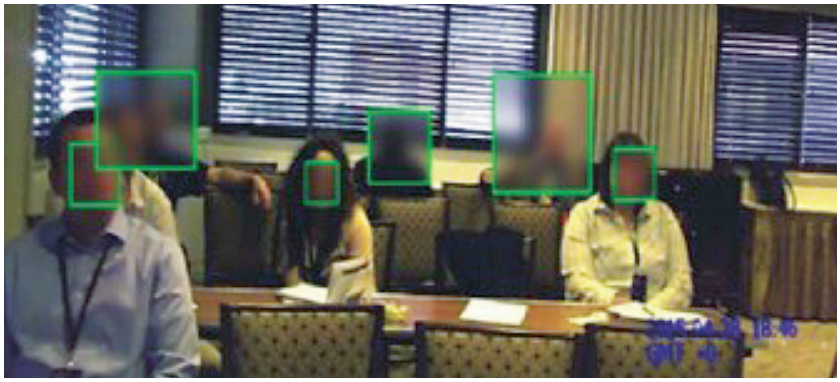
Because no single answer is sufficient, we have found it necessary to take a broad spectrum approach to developing situation-specific answers to this question and implementing those answers effectively in our cloud services. Privacy laws and regulations vary tremendously in their scope and definitions from one country or industry to another. Similarly, many

different technical standards are relevant to the protection of personally identifiable information (PII).

A compelling example of why cloud providers need to deploy specific privacy standards to protect sensitive PII comes from a customer who recently chose to deploy its applications on Microsoft Azure. The customer is TASER, a well-known supplier of law enforcement equipment. In recent years, TASER has become the world's largest supplier of police body-worn cameras. Now being deployed in the thousands by law enforcement agencies across the United States and in other large markets such as the UK, these cameras generate enormous quantities of video data on a continuous basis. As a practical matter, the only affordable and technically feasible place to store this video data is in the cloud. This is why TASER made the decision early on to bundle its body-worn cameras with its own cloud video storage and retrieval service called Evidence.com.

Video from police body cameras is not inert matter. It is live evidence that is subject to strict legal rules governing access rights and the chain of custody. It must be readily searchable and made available for review by multiple participants in law enforcement cases, including investigating officers, prosecutors, defense attorneys, victims and their families, elected officials, and often the media. But by its nature, police video frequently records scenes of individuals in states of distress that are not suitable for unrestricted distribution to the public. Hence, law enforcement agencies using body cameras have found it essential to develop video redaction policies to protect the privacy and identities of individuals captured on video, particularly when these individuals are victims, innocent bystanders, or vulnerable witnesses.

But the obligation to redact police video prior to public disclosure (as mandated by law in many states) creates a new problem. It turns out that manual video redaction is a very labor-intensive process, one that is so expensive that some law enforcement agencies have been forced to halt body camera deployments due to lack of staff and budget for redaction. Here is where cloud-based machine learning comes in. TASER decided to use machine learning capabilities available on Microsoft Azure that—under the supervision of a human expert—automate video redaction by recognizing individual faces and tracking them through extended video sequences.



Automated Redaction of Faces in Police Video (image source: Microsoft)

Yet one vital question remained. If TASER was not only to store vast quantities of sensitive police body camera video in the Microsoft Azure cloud, but also to use machine learning to identify and track individuals in that video in order to protect their privacy, what standards would ensure that this data would not be subject to share the encryption keys with Microsoft in order for Azure's machine learning algorithms to be applied to the data. Given this, what binding guarantees of conformity to rigorous standards could Microsoft offer TASER and TASER offer to its law enforcement customers that would assure the protection of data once it was transmitted from TASER's premises to Microsoft's data centers?

"Office 365 and Azure services were the first commercially available public cloud services to achieve CJIS compliance."

The answer to these questions lies in a little-known but crucial data protection standard specifically developed for sensitive law enforcement information. That standard is the FBI's Criminal Justice Information Services (CJIS) Security Policy.

Half a dozen years ago, when the cloud was still in its infancy, cloud providers were not well-versed in the unique data protection requirements of law enforcement agencies. In several cases, police departments were forced to cancel deployments of cloud-based email services when they discovered that the services did not comply with the CJIS Security Policy. We at Microsoft knew that we were not immune to similar setbacks. Accordingly, we took these incidents as a wake-up call and initiated a multi-year journey that culminated in our Office 365 and Azure services becoming the first commercially available public cloud services to achieve CJIS compliance.

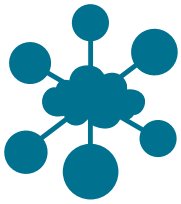
Meeting the CJIS standard required careful reengineering not only of the technical security features of our cloud services, but also of the business processes and personnel management practices in which those

services are embedded. To cite just one example, the FBI's demanding requirements specify that if employees of organizations providing services to law enforcement have access to protected data, they must pass rigorous criminal history background checks. Subjecting our data center personnel to such CJIS checks on a routine and institutionalized basis is an expensive process. However, we made the decision to accept this cost because we understood that it was an essential step towards meeting the needs of the broader state and local government community, of which law enforcement is only one—albeit crucial—part. Although the CJIS background checks are specific to our Government Cloud offerings in the United States, the business processes we developed to comply with this standard have had a positive spillover effect on all of our enterprise cloud services.

HOW ONE CLOUD PROVIDER IS MEETING THE CHALLENGE OF EU DATA PROTECTION LAWS

Big data applied to personal information can readily fall afoul of EU data transfer rules

Big data analytics will revolutionize the ability of enterprises to understand exactly what is happening in their markets and how to shape future outcomes. Such methods require enterprises to store and analyze vast quantities of data—so vast that the accepted term is "data lakes." Realistically, such "lakes" of data can only be stored in the cloud. Yet in many cases they will contain PII of customers and employees and will therefore fall under the strictures of data privacy laws, including the demanding new data protection laws recently passed by the European Union.



Question: How can multinationals doing business on both sides of the Atlantic ensure that their strategic big data analytics programs will not run afoul of rules governing international data transfers?

Answer: Multinationals should partner with cloud vendors who have spent years understanding what regulators require and how to implement both the technical and the legal components of a full-spectrum cloud compliance strategy.

At a time when technology has outpaced existing legal frameworks that govern how confidential data is protected, and when governments are struggling to balance public safety with the right to privacy, enterprises must work continuously to ensure that the services provided by their technology vendors retain the trust of all stakeholders—including governments, corporations and individual consumers. Recent events demonstrate just how complex this challenge can be for enterprises that operate in multiple jurisdictions.

Anticipating Compliance Changes

2000

Safe Harbor decision established that U.S. company self-certification for storing customer data complied with EU Data Protection Directive

2010

Microsoft starts developing "model clauses" as an added compliance safeguard without Safe Harbor

2015

Safe Harbor invalidated by the Court of Justice of the EU (CJEU)

In October 2015, the Court of Justice of the EU ("CJEU") abruptly invalidated U.S.-EU Safe Harbor Framework, which was based on a 15-year-old agreement between the United States and the European Commission that had enabled thousands of enterprises to move personal information across the Atlantic while remaining in full compliance with the EU's stringent data protection rules. But with the stroke of a pen, the CJEU threw the legality of transatlantic data transfers into doubt.

At Microsoft, we had long recognized that a sudden collapse of Safe Harbor was a possibility and had already taken steps to prepare for it. Starting in 2010, we assigned a dedicated team of several dozen lawyers and public policy professionals to the task of creating a new cloud contract based on the standard contractual clauses—often known as "model clauses"—that the Commission established pursuant to the EC's 1995 Data Protection Directive. Such an enhanced contract was not something we were required by law to offer, but we knew it would allow our customers to stay in compliance with EU law—at least provisionally—even without Safe Harbor.

Over a period of several years, our compliance experts met on numerous occasions with officials from the European Commission and the EU's 28 member-state Data Protection Authorities (DPAs) to hammer out a solution. In April 2014, the European DPAs determined that the Model Clauses in our new enterprise cloud contract met their requirements for a valid legal framework governing international data flows.[5] These clauses, which we now offer by default to all cloud customers of different sizes, ensure that even without Safe Harbor, all personally identifiable

5 See "Privacy authorities across Europe approve Microsoft's cloud commitments," Microsoft President and Chief Legal Officer Brad Smith, April 2014 (http://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/#sm.0001fb0wq4aepf5at9510wnbemw62) and "Article 29 Data Protection Working Party Letter to Microsoft," April 2014 (http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf).

“…it is critical for compliance professionals and in-house counsel to understand that compliance will always remain a moving target.”

information stored in the Microsoft cloud continues to meet Europe’s rigorous privacy standards no matter where it is located.

We undertook this complex and frankly quite expensive process because we knew that our cloud customers depend on their ability to use Microsoft services to transfer data across the Atlantic in a manner that complies with EU law. It was our job to anticipate future problems and to make certain that our customers could rely on stable and legally compliant cloud services, even in the face of an uncertain legal landscape subject to sudden tectonic shifts in prevailing regulatory regimes.

However, it is critical for compliance professionals and in-house counsel to understand that compliance will always remain a moving target.[6] The EC model clauses we introduced in our standard cloud contracts are themselves under challenge and may give way to new regulatory requirements. For example, the U.S. government and the EU have recently negotiated a new agreement called Privacy Shield to replace Safe Harbor. This is an important step toward creating a new legal framework to enable data to move between Europe and the United States in way that satisfies the data privacy and security concerns of both sides. The Privacy Shield has been ratified by the European Commission and all EU member states,[7] but it is nonetheless certain to be challenged in court.

Today, Microsoft is working with EU data protection authorities to ensure that its cloud services meet the requirements of the Privacy Shield. At the same time, recognizing that certain nations have data sovereignty requirements that go beyond Privacy Shield, Microsoft has also established data centers operated by trusted partners in countries such as Germany to offer customers an added layer of regulatory compliance assurance.[8]

---

6 For a review of developments as of June 2016, see “Privacy Shield and the General Data Protection Regulation: More Key Developments,” Sidley (http://www.sidley.com/news/2016-06-02-privacy-update).
7 See “Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield,” July 8, 2016 (http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm).
8 For example, in November 2015 we announced plans to open two new data centers in Germany operated under an innovative “data trustee” model that guarantees data sovereignty under German and EU law. These new facilities will offer standard Microsoft cloud services such as Azure and Office 365, but will be under the control of T-Systems, a subsidiary of Deutsche Telekom, an independent German company acting as a data trustee. Microsoft will not be able to access this data without the permission of customers or the data trustee, and if permission is granted by the data trustee, will only do so under its supervision (https://news.microsoft.com/europe/2015/11/11/45283).

Regardless of the outcome for Privacy Shield in its current form, it will be necessary for enterprises large and small to continue to grapple with changes in their legal and compliance requirements as they affect the use of cloud and other technology services. They should therefore actively seek out providers that will work to anticipate future legal and regulatory challenges and that are committed to deploying both the legal and engineering expertise needed to address these compliance challenges.

WHEN NECESSARY, CLOUD PROVIDERS MUST STAND UP TO GOVERNMENTS

"We have not hesitated to challenge the U.S. government when we believed this was necessary to protect the interests of our customers and to preserve the rule of law."

A cloud provider's commitment to stand with its customers in matters of legal and regulatory compliance is every bit as important as its promise to offer the latest technical features and functionality. This commitment goes further than simply anticipating changes in the regulatory environment. When circumstances warrant, it also means that the cloud provider must be ready to challenge government actions in court that threaten the legitimate privacy and security interests of its customers.

At Microsoft, we have not hesitated to challenge the U.S. government when we believed this was necessary to protect the interests of our customers and to preserve the rule of law. In recent years, we have gone to court on multiple occasions to challenge government actions or demands that, in our view, exceeded what is permissible under existing law. In one of these cases, we won the right to disclose government requests for data held by our corporate customers. And while the vast majority of business users will never be the target of such a request, Microsoft fought to ensure that our customers' right to know what happens to their data is recognized and preserved as a matter of law and principle.

In a more recent case, the U.S. government demanded that Microsoft turn over emails of a customer who is not an American citizen and whose emails were stored in our data center in Dublin, Ireland. We believed that

this unilateral attempt to exercise extraterritorial power to seize private information from a U.S. cloud provider operating overseas went beyond the intent of U.S. law and instead should have been pursued directly with the government of Ireland, in accordance with existing international agreements. We are proud to say that we received overwhelming support for our stand from many technology companies, legal experts, and privacy advocates, as well as from the government of Ireland and several members of the European Parliament.[9] On July 14, 2016, the United States Court of Appeals for the Second Circuit issued a historic decision in our favor, ruling that:

Microsoft quickly responded and legally turned over email data from suspects' accounts during Paris terrorist attacks in November 2015

…the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers.[10]

Our willingness to stand up for the rule of law and the preservation of privacy extends to support for our competitors as well. In March 2016, we joined with a number of other leading technology firms to file a legal brief in support of Apple, as that company fought an FBI demand that it implement extraordinary measures to defeat the encryption on an iPhone used by one of the shooters in the terrible terrorist killings of December 2015 in San Bernardino, California.[11]

Of course, balance is essential in matters of public safety and national security. We take very seriously our responsibility to work with both American and foreign law enforcement agencies to help keep the public safe in accordance with the law. We have demonstrated this on a number of occasions by responding swiftly to urgent lawful requests for information. For example, when French police were pursuing fugitives following the Paris terrorist attacks in November 2015, we were able to turn over email data from the suspects' accounts within 45 minutes of receiving the request. But we also know that people won't use technology that they don't trust. Undermining these protections will only put us all at greater risk.

---

9 "Business, Media and Civil Society Speak Up in Key Privacy Case," December 15, 2014 (http://digitalconstitution.com/2014/12/business-media-civil-society-speak-key-privacy-case/).
10 U.S. Court of Appeals, "In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation," July 14, 2016 (https://consumermediallc.files.wordpress.com/2016/07/14-2985_complete_opn.pdf).
11 "Brief of Amici Curiae Amazon.com, Box, Cisco Systems, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, WhatsApp, and Yahoo in Support of Apple, Inc.,"
March 22, 2016 (http://images.apple.com/pr/pdf/Amazon_Cisco_Dropbox_Evernote_Facebook_Google_Microsoft_Mozilla_Nest_Pinterest_Slack_Snapchat_WhatsApp_and_Yahoo.pdf).

STANDARDS ARE ESSENTIAL FOR TRUST IN THE CLOUD

“Neither encryption nor customer audits can provide a fully satisfactory response to the compliance challenge.”

The crux of the cloud compliance challenge lies in the fact that customers who choose the cloud must potentially place vast quantities of sensitive data into the hands of third parties whose facilities they do not control, often subject to the stringent regulatory requirements of specific sectors (banking, healthcare, government, consumer and employee PII, etc.). At the same time, customers must entrust these outside providers with the mission-critical business applications that process this data.

One might think that end-to-end data encryption or thorough onsite inspections of cloud provider data centers would mitigate some of the risks for customers. However, given the nature of cloud computing, neither encryption nor customer audits can provide a fully satisfactory response to the compliance challenge.

Regarding encryption, while it is technically feasible for a user to encrypt data before sending it to the cloud and to ensure that the provider does not have access to the encryption keys, this approach is often not practical on a large scale. For example, while some large users in sensitive sectors do install special equipment to encrypt cloud-bound email, such encryption cannot conveniently be applied to email exchanged with correspondents outside the organization’s own firewalls, and in any case the metadata associated with the email (such as destination addresses) cannot itself be encrypted. Furthermore, sophisticated cloud-based algorithms such as machine learning, as well as security routines such as malware detection, cannot work on encrypted data thus limiting the value of the cloud for customers.

Engagement of leading third-party auditing firms ensure compliance to literally dozens of formal standards

Allowing every customer the unfettered ability to conduct onsite inspections of cloud data centers would raise a host of practical challenges. At Microsoft, we have over 200 data centers around the world, including approximately a dozen that classify as true hyper-scale facilities. We subject all of these facilities to rigorous technical and business process engineering and regularly engage leading third-party auditing firms to ensure our compliance with literally dozens of formal standards. It would be impossible to manage thousands of customers

continually arriving to inspect these sites and audit their regulatory compliance. To do so would, in fact, constitute a serious security risk that would be against the best interests of our customers.

But the inadvisability of having individual customers audit cloud facilities points to the central importance of delegated trust provided by rigorous and widely recognized formal standards that are certified by independent third parties.

Examples of some of the many established standards Microsoft's cloud services comply with[12]:

Global

- International Standards Organization: ISO 27001/2 (general IT security)
- ISO 27018 (protection of PII stored in the cloud)
- Cloud Security Alliance (Cloud Controls Matrix 3.0.1)

Regional or National

- Argentina's PDPA
- Australia's IRAP
- China's MLPS
- Europe's ENISA Information Assurance Framework
- Japan's Cloud Security Mark

Industry/sector specific

- U.S. Federal Government's FedRAMP
- Healthcare sector's HIPAA
- Financial industry's PCI-DSS
- Financial industry's SOC 1
- Financial industry's SOC 2

"Microsoft has created a large dedicated organization of specialists whose full-time job is to manage the year-round standards audit activities that are continuously underway at our numerous data centers."

Virtually every one of these standards, and many others, require rigorous annual audits of our facilities or capabilities by accredited auditors. Complying with these multiple inspection and audit requirements is a resource- and time-intensive process that user enterprises would find extremely challenging to implement for their own data centers. In order to meet these requirements at Microsoft, we have created a large dedicated organization of specialists whose full-time job is to manage the year-round standards audit activities that are continuously underway at our numerous data centers.[13]

These teams must ensure coverage of complex requirement sets and manage frequent changes that result from the changing landscape of regulations, statutes, standards, and industry best practices for cloud services. As part of this work, we have created a standard methodology for defining compliance domains, determining which objectives apply to a given team or asset, and capturing how domain control objectives are

12 For a complete catalogue of standards implemented by our cloud services and extensive background information on each standard, see our recently launched cloud compliance portal at http://www.microsoftcloudassurance.com/.
13 For details of this process, see "Microsoft's Compliance Framework for Online Services" (download.microsoft.com/download/0/4/9/049F6894-3B22-4EC6-8DBD-E4FA27019820/Microsoft_Compliance_Framework_for_Online_Services.pdf).

addressed as they apply to a given set of industry standards, regulations or business requirements.

This highly structured approach is essential to giving us a clear understanding of the control activities that our cloud infrastructure teams must accomplish, the reasons behind each control activity (e.g., the specific clause from a requirements document such as SOC 2, or the specific element of security policy that drives the need to perform the control activity), as well as other functions that allow us to effectively manage our compliance programs. These programs also include frequent self-reviews performed by our internal teams and outside reviews of our overall performance against the control objectives. The reports prepared by third parties that conduct the regular audits of our cloud infrastructure provide a scalable mechanism for us to communicate our compliance capabilities to our customers and partners.

This compliance model extends to Microsoft's consumer as well as enterprise cloud services, allowing for trusted third parties to examine service elements and provide detailed reviews of specific services such as Office 365 and Microsoft Azure. These independent assessments are logically stacked upon one another to reflect dependencies, and summary reports of these assessments are shared with our customers and partners.

We believe that this approach to managing our compliance program and control framework is essential if we are to continue to provide trustworthy cloud services.

BUILDING A FRAMEWORK FOR TRUST

While cloud computing opens tremendous new opportunities, it also introduces great uncertainty. The same capabilities that make the cloud such a powerful enabler of commerce, connection and innovation can also be used to threaten our most fundamental rights and values. The bulk collection of personal information by U.S. and foreign intelligence agencies, recent terrorist attacks in the United States and Europe,

the European Court of Justice decision to strike down the Safe Harbor Agreement—all these events raise important questions about privacy and safety, and make clear that technology needs to be governed by the international rule of law, not just the laws of physics and not just the laws of the United States.

At the heart of these questions lie matters of trust. As citizens, we want to trust that our governments can keep us safe and protect our right to privacy and free expression. As consumers, we expect technology to respect our preferences and keep its promises. As businesses, we need to be confident that we can serve our customers while obeying the laws of the countries in which we operate. For members of the legal and compliance community, trust is especially important to ensure that their clients meet regulatory obligations and community expectations while reaping the economic and strategic benefits of the cloud.

Microsoft's corporate mission—to empower every person and every organization on the planet to achieve more—depends on our ability to win and retain our users' trust. We strive to build trust through our commitment to principles that reflect timeless values that we share with all stakeholders. After long experience grappling with these issues, we reached the conclusion that such trust cannot be built in an ad hoc way. It must be built brick by brick on a deliberately designed and constructed foundation of first principles. After an extensive process of internal discussion and analysis, we have made the commitment to build all Microsoft cloud services on the following four fundamental pillars:

Security

Our priority is to safeguard your data with state-of-the-art technology, processes, and encryption.

Privacy and Control

Your data is your data, you own it, you control the privacy of your data, who has access to it, and where it resides..

Compliance

We will always offer the largest portfolio of compliance standards and certifications in the industry.

Transparency

You will always have complete visibility into where your data is located and how it's managed.

We believe that these principles and our commitment to them set us apart. But we also know that we need to demonstrate exactly what these principles mean in practice for the legal and compliance community. And we understand that it is our responsibility to provide tools and information that will enable you to deploy our cloud services with the highest confidence that they are safe and compliant. For us, that is why compliance is a carefully engineered product, just like software code itself.

"Microsoft has more than 1,400 lawyers and public policy professionals working with legal and compliance leaders to help you tackle the regulatory issues you face…"

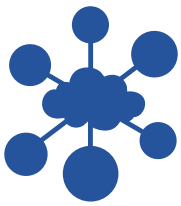
Our commitment to the legal and compliance community is deep and long-standing. It's the reason why Microsoft has more than 1,400 lawyers and public policy professionals working with legal and compliance leaders to help you tackle the regulatory issues you face in more than 100 countries where you and we do business.

Our work on Model Clauses is not the only example of our commitment. We were

the first cloud provider to offer Business Associate Agreements that enable healthcare organizations to comply with HIPAA. We were the first to meet the FBI's Criminal Justice Information Services data protection standard for law enforcement data. In education, we were the first major cloud provider to commit to the Future of Privacy Forum's Student Privacy Pledge. In the financial sector, we have done more to meet the exacting compliance needs of the world's biggest banks than any other technology company, which is one reason many of the world's leading financial institutions are adopting our cloud services.[14] And we were also the first cloud provider to achieve compliance with ISO's crucial new 27018 cloud privacy standard.

14 For recent examples of how banks are working with our cloud services and dedicated compliance program for the Financial Services sector, see "Helping banks get more out of applications, the cloud and big data: Microsoft at Sibos 2015" (http://blogs.microsoft.com/transform/2015/10/15/helping-banks-get-more-out-of-applications-the-cloud-and-big-data-microsoft-at-sibos-2015) and "Transparency and assurance: How Microsoft is helping financial institutions move confidently to the cloud" (http://blogs.microsoft.com/transform/2015/10/13/transparency-and-assurance-how-microsoft-is-helping-financial-institutions-move-confidently-to-the-cloud).

Trust is critical in your work and in ours. For your organization to succeed, you must be able to deploy technology solutions that your employees and your customers trust. And to fulfill our mission to empower every person and every organization, we know that earning your trust each and every day is critical. In the months and years ahead, we look forward to working in close partnership with you to achieve our common goal of ensuring that trust lies at the heart of technology.



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 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (EU General Data Protection Regulation).

against: a company able to deal effectively with the requirements of the EU Data Protection Directive[1], and, coming into effect in May 2018, the EU General Data Protection Regulation or GDPR[2], will likely be able to satisfy data privacy laws in other jurisdictions as well. In this sense, the EU Genetal 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 the EU Genetal 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. The EU General Data Protection Regulation, which will come into effect in May 2018, provides for a more detailed list of requirements of the data processing agreement than the currently applicable 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 Privacy Shield arrangements, EU Standard Contractual Clauses or Binding Corporate Rules (BCR), as may be appropriate in the individual cases. The Privacy Shield Decision replaces the previous Safe Harbour framework, which was the basis for transfer of personal data between US and the EU until it was struck down by the CJEU in October 2015. European Commission Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council, on the adequacy of the protection provided by the EU-U.S. Privacy Shield (the "EU-US Privacy Shield Framework"), which covers the specific case of personal data transfers to certified entities

included on the Privacy Shield List, replaced the Safe Harbour framework which was declared invalid by the European Court of Justice on 6 October 2015. 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.

In the light of the developments in recent years in relation to transfer of personal data to the USA, the key mechanism for cross-border data transfers to third countries which do not offer a level of personal data protection corresponding to the EU level, have been undoubtedly the so called EU Standard Contractual Clauses[3]. In the view of the Article 29 Data Protection Working Party, 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 AND ISO/IEC 18086-1:2016: FIRST PRIVACY-SPECIFIC INTERNATIONAL STANDARDS 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 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 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.

ISO/IEC 19086-1:2016 In addition to the above mentioned ISO 27018 standard, a new standard has been recently developed for cloud service level agreements (SLAs), the ISO/IEC 19086. This new standard provides for a framework for both organizations thinking about migrating to cloud computing as well as for cloud providers. In 2016 the first part of the standards, ISO/IEC 19086-1:2016 has been released. This part includes an overview of SLAs for cloud services with basic information and explanations of concepts, aims and terms commonly used in the cloud computing environment. The following three parts - ISO/IEC 19086-2, 19086-3 and 19086-4 - will define further requirements on security and privacy aspects, conformance requirements or metrics for cloud SLAs. These remaining parts of the ISO/IEC 19086 are still under development and are expected to be released in near future.

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

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

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;[4] they share source codes to help customers reassure themselves that there are no 'back doors' through which state authorities would access their data, and strengthen encryption, among other measures. In order to guarantee a maximum security that cloud customer's data will not be handled arbitrarily and without his knowledge, it is appropriate to agree with the cloud provider on detailed rules covering such requests and embed an obligation of the cloud provider to ascertain that the relevant state authority is indeed entitled to perform the given power.

CLOUD IN SPECIFIC SECTORS

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

It has become common for large, multinational cloud providers to certify their data processing operations and facilities; in this regard, the 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.[5] 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.

5 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 General Data Protection Regulation foresees a considerable change it is explicitly mentioned.

INTRODUCTION

1

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

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

There is currently no conclusive decision or guidance on the EU level on when encrypted data may be safely regarded as anonymized data and thus

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

outside of scope of personal data protection[2]. The General Data Protection Regulation explicitly regulates the use of anonymized data, when it 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.

The CJEU provided some guidance on the scope "means reasonably likely to be used for decryption" in its Case C-582/14, Breyer, issued on 19 October 2016. The CJEU considered a dynamic IP address to be data relating to an 'identifiable natural person' and thus constituting personal data, although data needed to identify natural persons are in case of dynamic IP addresses held by various parties (in this case the online services provided and the internet connection provider) and none of the parties alone is able to identify the natural person without the data held by the other party.

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.

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.

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

3

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

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

A cloud provider is generally considered a data processor who processes 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).

The General Data Protection Regulation provides for further requirements and stipulates a detailed list of conditions and terms to be included in the data processing agreement.

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 Privacy Shield: Transfers of personal data to US organizations adhering to the principles of Privacy Shield 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. Pursuant to Cloud Opinion and the recent developments in relation to the invalidated Safe Harbour framework, 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:

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/en/legislation/zakon-o-varstvu-osebnih-podatkov/

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.

The European Court of Justice in its ruling (Judgment in Case C-362/14) on 6 October 2015 declared the old Safe Harbour framework invalid. On July 12 2016 European Commission adopted the EU-U.S. Privacy Shield, which is the new framework that protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers. The EU-U.S. Privacy Shield is based on the following principles: Strong obligations on companies handling data, Clear safeguards and transparency obligations on U.S. government access, Effective protection of individual rights, Annual joint review mechanism. Detailed contents of mentioned principles available at http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

Under Privacy shield agreement (which has been in use since 1 August 2016) in Slovenia 4 key assurances for all individuals whose personal data are transferred in the United States must be fulfilled:

- processing of personal data must be based on clear, accurate and accessible rules/provisions: it means that any average informed person may be able to predict what might happen to his/her personal data after his/her personal data is transferred;

- necessity and proportionality of the data processing with respect to the legitimate purpose must be shown: balance between the aim of the collection and processing of personal data (in general, national security) and the rights of the individual needs to be found;

- an independant, unprejudiced and efficient control mechanism, which in practice operates efficiently needs to be established/ensured: either a judge or any other independent body, under condition that it has sufficient ability to implement the necessary control;

- effective remedies must be available for individuals: everyone should have the right to protect his/her rights before an independent authority.

The role of the Privacy Shield concept is that it allows the transfer of personal data from the EU to the company based in the United States if a latter company process personal data there (eg. uses, stores or transfer) in accordance with a set of strict data protection rules and safeguards.

All operators based in the EU (i.e. including operators from Slovenia), who transfer personal data to companies based in the United States, are now available/allowed to legitimately transfer personal data to the U.S. under/with the use of the mechanism provided under this arrangement (Privacy shield agreement), of course in addition to other available mechanisms. All operators based in the EU are now available to ensure the protection of personal data on the basis of the inclusion of a partnership company based in the United States into the scheme of the Agreement on a Privacy Shield EU. Additionally, a decision of the DPA is required for transfers under the EU-US Privacy Shield Framework since no entity yet has requested the confirmation of Privacy Shield before Slovene DPA.

This concept of a Privacy Shield has already been challenged in EU General Court, but is currently still in use.

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 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, Nos. 73/15 and 49/16*; hereinafter referred to as the "Decision") that has been adopted the Banking Act (Official Gazette of RS, Nos. 25/15 and 44/16 - ZRPPB) The Decision requires that the banks:

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

(ii) under new Banking Act (Official Gazette of RS, Nos. 25/15 and 44/16 – ZRPPB) in use as of 13 May 2015 this provision was deleted

(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. 93/15) requires insurance companies to adopt the Act determining approach to the outsourced business and respective procedures and 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. 77/11, 10/12 - Takeover Act 1C, 55/12, 96/12 - ZPIZ-2 31/15 - ZISDU-3) 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. 100/15), 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/novice/iso-standard-za-ponudnike-racunalnistva-v-oblaku-1295/

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/Smernice_Racunalnistvo_v_oblaku_povzetek_za_mala_podjetja_2016.pdf

PENDING LEGISLATION

14

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

No.