Personal data protection & cloud computing

INFORMATION COMMISSIONER
&
Cloud Security Alliance Slovenia Chapter
ISACA Slovenia Chapter
Zavod e-Oblak, Eurocloud Slovenia

Purpose of the document:	The purpose of the document is to establish common control points, by which **users** as well as **supervisory authorities** will be able to come to informed decisions regarding the use and oversight of the cloud computing services in part where processing of personal data is concerned. The initiatives for safer use and certifications of cloud services on the other hand are offered guidelines for future developments with the goal of compliance with personal data protection legislation.
Target public:	• Users of cloud computing – small and medium enterprises and organizations • (Local) providers of cloud computing • State supervisors for data protection • (certified) auditors of information systems • Internal and external auditors
Status:	public
Version:	1.0
Date of issue:	15.6.2012
Key words:	Guidelines, cloud computing, PDPA, personal data protection, security, privacy, transfer of data to third countries, contractual data processing, risk assessment, information security.

CONTENTS

ABOUT THE INFORMATION COMMISSIONER'S GUIDELINES

The purpose of the Information Commissioner's guidelines is to provide common practical instructions and procedures for data controllers in a clear and appropriate manner. It seeks to address the most common questions from the area of personal data protection that different data controllers are faced with. With the help of guidelines data controllers should accordingly be able to comply with the statutory provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07 – official consolidated text; hereinafter: PDPA). These specific guidelines are intended for the potential users of the cloud services, as well as for the supervisory, auditing, and counselling institutions.

The legal basis for the Information Commissioner (hereinafter: the Commissioner) to issue guidelines is provided by Article 49 of PDPA which authorises the Commissioner to give non-binding opinions, explanations and positions regarding personal data protection, and, further to this, publish these on its website or in other suitable formats, as well as prepare and offer instructions and recommendations regarding personal data protection in individual areas.

See also:

- Commissioner's opinions: http://www.ip-rs.si/index.php?id=383
- Commissioner's brochures: http://www.ip-rs.si/index.php?id=388

The Commissioner's Guidelines are published on the website: https://www.ip-rs.si/index.php?id=388.

1. INTRODUCTION

Cloud computing is promising access to computing facilities from any location, in an economical, adaptable and upgradable way, that is why it is not surprising that ever more organizations processing personal data are interested in its use. In this context doubts regarding compliance with data protection legislation are unavoidable. Especially with public models of cloud computing, where data protection issues are inherent to the nature of such model, there are specific risks regarding contractual data processing agreements, i. e. the outsourcing of service provision, information security and transfer of data to third countries which do not provide for adequate level of data protection. Cloud computing brings vast potential; however this should not lower the level of the right to data protection, a fundamental human right. This is also one of the main recommendations of the International Working Group for Data Protection in Telecommunications (IWGDPT) in the "Sopot Memorandum" on data protection in cloud computing[1]

In cloud computing the service providers are outside our direct control. The essence of lawfulness and at the same time practical acceptability of the service is therefore trust. The client, or the data controller, is the one who has to make a risk assessment, alone or with the assistance of adequately qualified third parties. Based on the results the client has to make a decision whether or not to trust a certain cloud provider. If a cloud provider is not able to provide the client with satisfactory information and assurances regarding security of the data, the client who correctly assesses the risks, should retain a certain level of cautiousness and restraint.

[1] IWGDPT: Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland): http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

The purpose of these guidelines is to raise awareness regarding the risks of data processing in the cloud, and to offer a clearer picture on current data protection legislation requirements with a control list. Information Commissioner believes that many cloud service providers currently do not offer their potential clients the information they need to conduct a proper risk assessment and that mechanisms need yet to be put in place that will allow for distinguishing the trust worthy providers from the ones that present higher risks. In times when many activities in the fields of standardisation, certification and other mechanisms for building trust in cloud computing are taking place, we hope, that these guidelines will offer some much needed help in decision making processes.

1. THE CONCEPT OF CLOUD COMPUTING AND THE MAIN CAHARACTERISTICS

Cloud computing is a form of information technology use where not much investment in efficient software is needed. Access to applications and services is enabled over the network and only access to internet connection is required. It is possible to access the cloud with the use of an ordinary client anywhere and anytime the user needs a certain information facility, without special software. Cloud computing offers the clients immediate access to pre-set common information resources (for example to the network, hardware, storage capacities, software, different information services) that are readily available without an extensive agreement making process. **Cloud computing can be described by 5 fundamental characteristics, 3 service models and 4 deployment models.**

2.1 Main characteristics of cloud computing

» Self-service on demand«
The user may decide on the use of computing facilities such as server time and network storage independently, on the basis of their current needs, without excess communication with different service providers.

Broad network access
Computing facilities may be accessed over the network through the use of standardised mechanisms that support different clients, such as mobile phones, tablets, laptops and work stations.

Combining of computing resources
Besides classical virtualization cloud computing uses also the capabilities of automation and orchestration of services and multi-tenancy of users at common information resources. Common use of the same technological resources is an essential feature of cloud computing. Before this a cloud provider had to establish divided infrastructures for different users, however with the rise of multi-tenancy mechanisms it is possible to provide homogeneous configuration, uniform control over the services, upgrading and simpler disaster recovery processes and restoring of the data. Another important feature is closely connected - the data are not necessarily tied to a precisely defined physical location anymore, because they can at the same time be located in a number of data centres, anywhere in the world.

High elasticity
The user may easily increase or decrease the computing capacities afforded based on the current requirements. The capacities are unlimited for the user.

Pay per use
The cloud system is automatically controlled and optimized based on the type of service (for example storage, processing, bandwidth, the number of active users). Transparency of the use of resources is achieved thorough control and monitoring.

2.2 Service models

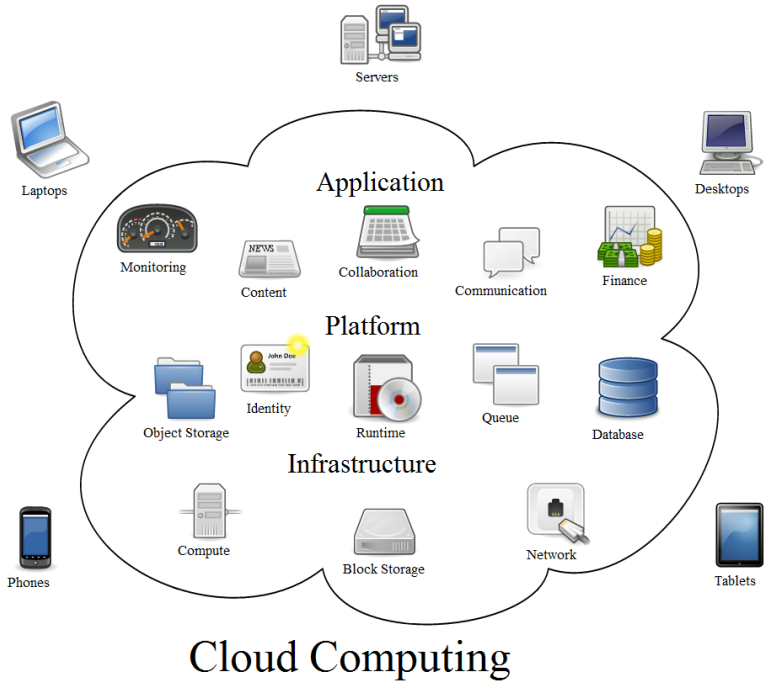
The **service models** refer to the type of service offered. The cloud service can be implemented in three different service models, usually built on top of each other that may also be used independently from one another.

Infrastructure as a Service – IaaS
Infrastructure as service refers to computing infrastructure, often offered with the use of virtualization. These are servers, storage, network, namely infrastructure as service (IaaS) – the common service providers[2] include so VMware, Oracle, IBM, Microsoft, KVM, OpenStack, Xen, Eucalyptus, Nimbus, OpenNebula,Citrix Cloud, AppNexus, Amazon EC2, etc.

Platform as a Service – PaaS
Platform as service already includes basic additional functionalities (usually in the form of an Application Programming Interface – API), which are used as a platform for development and use of users' own information solutions. Part of this category is application development environment, namely platform as a service (PaaS). Some known providers include Google AppEngline, Microsoft Azure, Oracle PaaS, IBM PaaS, VMware SpringSource, etc.

Software as a Service – SaaS
Software as service refers to provision of the complete infrastructure, together with the software and the settings for its use. In this category there are the functionalities of business applications, namely software as service (SaaS). Some known providers include salesforce.com, Microsoft (for example Office 365), Google Apps (including Gmail). With other words, all the user usually needs is a web browser and access to the internet. Everything else is provided by the service provider, in some cases even free of charge.

[2] A cloud taxonomy is available at: http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png.



Picture 1: An abstract scheme of cloud computing concept

2.3 Deployment models of cloud computing

The deployment models of cloud computing are the following:

Public clouds are publicly accessible, with no limitation on the type of users. These are the ICT services of the provider which can be accessed from anywhere with the internet connection.
Private Clouds are only accessible in a private network. ICT services are offered in the providers' data centre. All services, as well as infrastructure are under control of the provider, whereas management can be implemented through a third party. The services are available on the internet or over the virtual private networks.
Community Clouds are only accessible to a limited number of clients with known features.
Hybrid Clouds are ICT services in the cloud, composed by public and private clouds services.

The cloud service providers refer to a number of advantages cloud computing offers: from lower costs because of the lack of investment in, for example, hardware, to higher and faster adaptability to the needs of the client (you can acquire additional capacities when needed), and the alleged lower costs of maintenance, support and other services tied to the ICT human resources. In some models, often all you need is access to the internet and a web browser.

The fundamental characteristics of cloud computing may present an advantage as well as a weakness, but certainly cloud computing is connected with risks, not applicable to other forms of outsourcing of the ICT services.

3. CLOUD COMPUTING THROUGH THE BASIC PRINCIPLES OF PERSONAL DATA PROTECTION

3.1 BASIC POINTS

Pursuant to the provisions of the PDPA normally[3] the user or the **client** of cloud computing services would be in the role of a **data controller**, and the **cloud provider** in the role of its **contractual data processor**, performing certain tasks regarding data processing, such as storage, copying, transferring, etc. A reminder – any handling of personal data is regarded as data processing[4], and personal data are any information related to an identified or identifiable individual. Be cautious, even if you cannot tell by yourself, who the data is relating to, others may be able to identify the person, without disproportionate effort or means. Identifiabiliy of an individual should be interpreted broadly and not only through the capabilities of a certain entity, and through the presence of the exact data that enable direct identification of an individual.

Certain aspects of data protection, such as the proportionality principle, the purpose of data processing, and retention periods are, of course, an integral part of the framework for data protection. However, in the context of cloud computing they do not present any specificity. The areas that are exposed the most are the following:

- contractual personal data processing,
- data security,
- and transfer of data to third countries.

From the viewpoint of personal data protection cloud computing is addressed in the recently published opinions by the International Working Group on Data Protection in Telecommunications[5] and the Article 29 Working Party[6].

3.2 CONTRACTUAL PERSONAL DATA PROCESSING

A data controller may decide to entrust certain tasks regarding personal data handling to a contractual partner. Normally the client should decide, what the partner is commissioned to do and how, however the circumstances today are such, that normally the cloud providers are the ones to set the terms, the level of data security and other important aspects of business relationship. Nonetheless, the clients are the ones with appropriate legal grounds for data processing, and have determined the purposes and means of data processing; that is why **normally the clients are regarded as data controllers and the cloud providers as contractual data processors**[7]. Contractual data processing is therefore admissible under condition that certain

[3] In certain cases we can speak about joint controllership, especially when a provider processes personal data outside of the scope of the client's instructions. Certainly the provider may only do that on proper legal grounds. It is crucial that the client and the provider clearly define their roles.

[4] It has to be emphasised that even if the contractual processor cannot establish the identity of the individuals whose data it processes (such as in the case of mere storage of the data), its activity is still regarded as personal data processing. Even more, if the client stores its data at the outside provider's disc capacities, and the data are encrypted and thus unintelligible to the provider, the storage would still be regarded as personal data processing, and the client and the storage provider would have to comply with the respective legal obligations.

[5] Sopot Memorandum, accessible from: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

[6] http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

[7] Article 29 Working Party argues in its Opinion no. 1/2010 on controller-processor that »the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the

safeguards are put in place, foremost regarding the adequate level of data security on the side of the cloud provider, as well as on the side of its sub-processors. Article 11 of the PDPA provides that a data processor may perform individual tasks associated with processing of personal data within the scope of the client's authorisations, and may not process personal data for any other purpose. Mutual rights and obligations must be arranged by contract, which must be concluded in writing and must also contain an agreement on the security procedures and measures to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data (Article 24 of PDPA). Article 29 Working Party in its opinion on cloud computing addressed the necessary contents of the contract.

Here we come to the main question of the privacy advocates – if and when can (outside) cloud computing provider be trusted?

The clients often face general terms of service where the actual data controller is the party with less negotiation power, and can only accept or decline the general terms of use presented by the cloud service provider, even though the data controller should be the one to determine the purposes, circumstances, and means for data processing, and the requested level data security.

3.3 SECURITY OF PERSONAL DATA

Information security is a fundamental part and one of the essential principles of all the legal acts regulating the field of data protection. As a *narrower part of personal data protection* it refers to the protection of integrity, confidentiality and accessibility of personal data. Data security aspect was emphasised by the Danish supervisory authority for data protection which did not grant the permission to a certain municipality to transfer personal data to the cloud provider from the USA[8] on the grounds of doubts regarding security measures. A similar stand was taken by the Norwegian supervisory authority[9]. Whether personal data are better secured in the cloud is not an easy question and a general answer along the lines, that if something is under our control, it is more secure, is not satisfactory (ENISA[10], 2009). As some authors argue, it is foremost the question of trust (Schneier[11], 2009). Just as we have to trust an operation system, hardware, and software, we also have to trust providers of cloud computing – it is actually a similar service and just another provider, we have to judge from the aspect of trust. However, there is an important difference in outsourcing – if we have the computing capabilities under our control, we can, alone or in cooperation with other parties, take care of security with different security mechanisms (the files on the computer can be protected with back-up copies, antivirus programs, if we don't trust entirely a certain solution, such as a web browser or an operation system). On the other hand, we have to trust an outside processor entirely, which entails not only trust in its security procedures and measures, but also in its reliability, accessibility and continuity of its operations. If we carry out the processing ourselves, we need not worry that our competitor will buy our disc space, so that we would be forced over night to pay (more) for access to our own data. If we have adequate back-up copying policies in place, we do not worry about losing our data. If – and when – can we be sure about this in the

---

controller to accept clauses and terms of contracts which are not in compliance with data protection law«. The opinion is available at:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[8] A municipality wished to use Google Apps. Datatilsynet, The Danish Data Protection Agency: Processing of sensitive personal data in a cloud solution. Accessible at: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ (published 3.2.2011).

[9] http://datatilsynet.no/English/Publications/Will-not-let-Norwegian-enterprises-of-Google-Apps.

[10] ENISA: Cloud Computing Risk Assessment. Accessible at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (published 20.9.2009).

[11] Schneier, B.(2009): Cloud Computing. Accessible at:
http://www.schneier.com/blog/archives/2009/06/cloud_computing.html (published 4.6.2009).

cloud? We should not forget about the human factor either. Even with clear instructions, people tend to use shortcuts often (such as borrowing login data). On the other side – a valid question is, whether a small data controller has the capacities to ensure such level of data security, as can be provided by a large provider of cloud computing services, with all its resources and economy of scale?

A client must always be able to assess whether the offered services fit its needs and legal requirements. This cannot be done without:

- adequate and transparent information from the provider, and
- assessment of the risks accepting the offer might bring.

If a data controller is not able to conduct such a risk assessment by itself, it may make use of the services of third qualified parties, or standardization and certification procedures and certificates. The latter are currently still being developed. Often the data controllers do not have all the necessary information from the service providers on the some of the main elements of data security, such as traceability of data processing, destruction of data after the purpose of processing was achieved and the information on the actual locations of personal data. In such conditions it is hard for data controllers to execute appropriate risk analysis before the decision on the use of cloud services. Transparency of the cloud service providers is therefore essential – the clients need to be presented with information on locations where their data will be processed, on how integrity, confidentiality and availability of data will be achieved, if and in which countries the data will be processed, when and how the data will be destroyed after termination of the contact, which sub-processor will be employed and what will their tasks regarding data processing be, and so on.

3.4 TRANSFER OF DATA TO THIRD COUNTRIES

A special chapter of issues in ensuring the expected level of personal data protection features the questions regarding transfer of data to third countries, which (do not) ensure adequate or the same level of personal data protection, compared to the national frameworks.

Transfer of data to third countries refers to any supply of data from the data controller based in the EU Member States to **an entity outside of the EU**, or when access to the data is enabled to organizations, individuals, etc. from third countries outside of EU, even if the data is still physically located in the EU (Article 62 of PDPA).

Such **transfer of data outside of the EU member States** to countries which do not ensure adequate level of personal data protection is only permitted under conditions in 2. Chapter of the PDPA (Articles 63 to 71). Before the transfer the data controller in many cases has to apply for an authorisation by the Information Commissioner.

3.4.1 Transfer to a country which ensures adequate level of protection of personal data

The data controller may transfer the data to a **country which as such ensures an adequate level of protection of personal data.** The decision on the adequacy is made by the Information Commissioner, which authorizes the transfer on the basis of an application from a data controller. The Commissioner is bound to respect relevant decisions of the European Commission, which has already established, that the following countries ensure adequate level of protection: Andorra, Argentina, Australia, Canada, Switzerland, Faroe Islands,

Guernsey, Israel, Isle of Man, Jersey, USA (only in part of Safe Harbor framework, and passengers data)[12]. In such cases the Commissioner authorises the transfer, following a summary administrative procedure and puts the country on its list from Article 66 of the PDPA. If adequacy of the country has not been assessed by the European Commission yet, the Commissioner carries out the authorisation procedure and the adequacy procedure.

3.4.2 Transfer of data to an organization that ensures adequate level of personal data protection (SCC and BCR)

A data controller may also transfer its data **to a certain organization** in the third county, after receiving an authorisation from the Information Commissioner, **if the organization and the data controller ensure adequate level of data protection, foremost with contractual provisions, etc.** The data controllers have at their disposal the following instruments:

1. model clauses, prepared by the European Commission – standard contractual clauses,
2. multinationals may choose to be bound by »Binding Corporate Rules – BCR«, to ensure adequate level of protection, or
3. by another type of agreement or business regulations, that satisfy the conditions of adequate data protection.

Most often standard contractual clauses are used. **Standard contractual clauses** are regarded as a tool that ensures adequate level of personal data protection and at the same time fulfils the conditions provided by Article 11 of the PDPA, because they are in a form of a written contract between the data controller and the processor, which specifies mutual rights and obligations, and at the same time include the agreement on procedures and measures for security of personal data from Article 24 of the PDPA. The first model of SCC is aimed at transfers from the data controller to a data processor in a third country[13], whereas the second type is offered to a data controller wishing to transfer data to another data controller in a third county[14] which does not ensure an adequate level of personal data protection. SCC also address sub-processing and provide that a processor may entrust processing to a sub-processor, on condition that the data controller is informed about this and that the processor remains liable for any actions of the sub-processor(s)[15].

Also increasing is the use of another instrument - **Binding Corporate Rules – BCR.** BCR are an internal act of a multinational corporation, a group of members, where some might be located outside the EU, in third countries, which do not ensure adequate level of data protection. The internal act includes the corporation's policy regarding transfer of data to third countries, in compliance with the provisions of the Personal Data Protection Directive. When the BCRs are accepted by the data protection authorities (DPAs) in the EU Member States, they are regarded as a tool which ensures adequate level of data protection for the data being transferred inside the group of members of a corporation. **Transfer of data outside of the corporation is not possible on the basis of the BCR.**

---

[12] The list is available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[13] A model of standard contractual clauses and both annexes from the Commission Decision of February 5 2010 for transfer to processors in third countries is accessible at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:SL:PDF.

[14] A model of standard contractual clauses and both annexes from the Commission Decision of December 27 2004 for transfer of personal data to data controllers in third countries is accessible at: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Contractual_clauses__slo.pdf.

[15] See more information in the Commissioner's guidelines on transfer of data to third countries: https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/.

The purpose of the BCR is to simplify the procedures inside a corporation, so that there is free flow of data between the members of the corporation. Therefore it is not necessary to apply for an authorisation at a DPA in case of each transfer. The BCR have to be accepted by a lead DPA, and after that the corporation has to apply for further authorisation at all the relevant DPAs. Transfer of data on the basis of BCR is only permitted inside the group. If the corporation wishes to transfer data to an outside processor, it needs to frame this transfer separately (for example with SCC) and possibly apply for a separate authorisation at the competent DPA.

* A new mechanism, currently being developed, especially appropriate for the cloud providers, is **BCR for processors.** A cloud provider will be able to ensure the level of data protection with an internal act, compliant with the EU legal framework.

Transfer without the Information Commissioner's prior authorisation

1. The data controller does not have to apply for a prior authorisation if the third country is on the list of countries from Article 66 of the PDPA which fully or in part ensure adequate level of personal data protection, if those personal data are transferred and for those purposes for which an adequate level of protection has been found. The countries on the list are: **Switzerland, Croatia, USA in part where it concerns organizations certified as compliant with the Safe Harbor, and Republic of Macedonia[16].**

2. Prior approval is also not necessary in the situations from Article 70(1) of the PDPA. The exemptions however may only be applied in exceptional situations, therefore not for massive and frequent transfers of data. Prior authorisation is not necessary when:
    - so provided by another statute or binding international treaty;
    - the individual to whom the personal data relate gives personal consent and is aware of the consequences of such supply;
    - the transfer is necessary for the fulfilment of a contract between the individual to whom the personal data relate and the data controller, or for the implementation of pre-contractual measures adopted in response to the request of the individual to whom the personal data relate;
    - the transfer is necessary for the conclusion or implementation of a contract to the benefit of the individual to whom the personal data relate, concluded between the data controller and a third party;
    - the transfer is necessary in order to protect from serious danger the life or body of an individual to whom the personal data relate;
    - the transfer is performed from registers, public books or official records which are intended by statute to provide information to the public and which are available for consultation by the general public or to any person who demonstrates a legal interest that in the individual case the conditions provided by statute for consultation have been met;

3.4.3 Transfer to the USA on the basis of Safe Harbor Principles

The Commissioner decided that the USA are partly ensuring adequate level of personal data protection in part considering the organizations that have certified its compliance with the Safe Harbor framework. European

[16] The list is available at the Commissioner's website: https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/seznam-tretjih-drzav-66-clen-zvop-1/.

data protection legislation differs significantly from the one in the USA, where some of the biggest cloud providers are based. International agreements, such as the Safe Harbor framework, provide for simpler transfer of data between the two different regimes. Safe Harbor enables data controllers to transfer their data to entities in the USA (such as Google, Amazon, etc.), if those entities have certified their compliance with the Safe Harbor principles[17]. To gain the benefits of Safe Harbor, an organization from the USA has to self-certify its compliance with the principles with the US Department of Commerce. This way an organization is bound to respect the Safe Harbor Principles and to declare this in its privacy policies. A list of certified organizations can be found on the Department of Commerce website: www.export.gov/safeharbor/.

The Commissioner decided[18] that the USA are ensuring adequate level of personal data protection in the part considering the organizations that have certified its compliance with the Safe Harbor Privacy Principles, published by the US Department of Commerce on July 21 2000. According to the European Commission Decision 2000/520/ES certification with the Safe Harbor Principles is regarded as an assurance that the organization ensures adequate level of data protection.

If data controllers wish to transfer data to an organization under Safe Harbor, they do not need to apply for an authorisation by the Commissioner, however it has to be emphasised that the sole certification with the Safe Harbor framework does not necessarily mean that all the legal requirements for such transfer are met. **The data controller and the processor have to also respect Articles 24 and 25 of the PDPA, which define data security.** The questions regarding compliance with security provisions, especially in the public clouds, and regarding adequacy of assurances offered by the Safe Harbor remain open. **The Commissioner believes that the data controller and the processor have to fulfil the requirements regarding data security from Article 24. of the PDPA. Even if the data controller may transfer the data without a prior authorization, it can still breach the provisions on data security from Article 24 of the PDPA.**

The Commissioner emphasises that currently many providers of cloud services do not seem to provide the procedures and measures for data security according to Article 24 of the PDPA, even though they are convinced that the sole certification with Safe Harbor ensures compliance with Article 24 of the PDPA.

Data controllers wishing to use the cloud services therefore have to pay close attention to the following obligations in the PDPA:

- regarding contractual personal data processing (Article 11),
- regarding data security (Articles 24 and 25),
- regarding transfer of data to third countries (Articles 63 to 71).

[17] More information on the Safe Harbor framework can be found here (available in Slovene language): https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/iznos-osebnih-podatkov-v-tretje-drzave/safe-harbor/.

[18] Decision no. 0601-2/2010/5.

Cloud computing brings certain specific risks, not raised by »ordinary« outsourcing, namely (according to the PDPA terminology) contractual personal data processing. The risks are well addressed by the ENISA report; to mention just the following:

- *Unequal bargaining power (provider – users),*
- *poor transparency of the providers,*
- *unclear location of data,*
- *disclosure of data to law enforcement, industrial espionage,*
- *»multi-tenancy«,*
- *decreased data portability,*
- *inadequate level of isolation of resource co-users,*
- *incapacity to monitor implementation of security policies,*
- *inadequate, imperfect or inefficient deletion of data,*
- *misunderstandings regarding the transfer of responsibility to the provider,*
- *decreased impact on the management of data,*
- *termination of service or the provider,*
- *takeover of the provider, together with the data,*
- *misuse of special (highest) access rights,*
- *abuse of service management interface/console,*
- *disclosure of data during transfer,*
- *data leakage when uploading/downloading or inside the cloud,*
- *disclosure or loss of the encryption keys, and*
- *inconsistencies in data protection at the provider and the client (most often at the client side)*

4. CONTROL LIST FOR COMPLIANCE CHECK

As we already explained, the purpose of these guidelines is to **raise awareness about the risks presented by processing personal data in the clouds** and to offer a control list, by which a data controller can assess its compliance with the requirements of the Personal Data Protection Act.

How to use the control list?
Some requirements of the controls need to be fulfilled by the client (marked with »C«), some by the provider (marked with »P«), and some by both of them (it is a question of responsibility or duty). The control list presents **mandatory controls, namely the minimal requirements of the law**. If these cannot be fulfilled you are **advised not to use the cloud services.** At each control there is a full description of the control in the notes column. For further assistance regarding the assessment of the services, the risk assessment, and other methodological tools, we recommend the use of sources and references listed in the last chapter.

How <u>NOT</u> to use the control list?

- The control list focuses on personal data protection requirements that are specific for the cloud environment. If you fulfil all the control requirements, that does not mean you have fulfilled all the obligations you may otherwise have as a data controller according to the PDPA (such as to define the persons responsible for individual filing systems, to respect retention periods, etc.).
- The control list should be used by the client as well as by the provider of cloud services – simply forwarding the list to the (potential) provider, who should fulfil it, is not appropriate.
- The real life cases and examples should not be interpreted as final, and the facts of a specific case should not be applied widely to all situations.

Number	Control list	YES	NO	C	P	Guidelines how to fulfil the control	Legal reference
	Personal data processing - general						
1	The client has legal basis to process personal data.	☐	☐	x		The client may only process personal data and transfer it further on appropriate legal grounds (such as consent of the individual or if provided by law), that means, before it decides on the use of cloud services. The legal bases are provided by articles 8 to 10 of the PDPA.	Articles 8, 9 and 10 of the PDPA
2	The client knows which categories of data will be transferred to the cloud.	☐	☐	x	x	The client has to know in every phase which categories of data are being transferred to the cloud; this can be represented by filing system catalogue or a data model. The client has to acquire in advance specific information on the categories of data that will be collected or further processed by the service provider's information system (relevant especially for the SaaS, where the client could be faced with the information regarding the necessary categories of data after it starts using the service).	
3	The provider fulfils all the criteria regarding the use of service a client requires.	☐	☐	x	x	The control can be fulfilled by standard contracts and terms of service, but only if they comply with the requirements of the client. Even if the provider does not adapt to the requests of clients, but fulfils all the criteria (of the client and the legal criteria). The client has to be cautious about contractual provisions on unilateral changes of the terms of service during service provision, and has to be prepared to change the provider if the original one changes the conditions in a way	Article 11(2) of the PDPA (to process data within the scope of the client's authorisations)

Number	Control list	YES	NO	C	P	Guidelines how to fulfil the control	Legal reference
						incompatible with the client's requirements. The client has to be informed on intended changes so it can terminate the contract if it does not agree with the changes.	
	Contractual personal data processing						
4	The client concluded a contract in writing with the cloud service provider.	☐	☐	x	x	The contract may be in electronic form, legally admissible and equal to written (see Electronic Commerce and Electronic Signature Act) The contract should include the recommended safeguards (see Article 29 opinion on cloud computing).	Article 11(2) of the PDPA
5	The contract in writing includes specific agreement on the procedures and measures for data security.	☐	☐	x	x	The agreement on data security can be a part of the contract or the general terms of service or it can be a document added to the contract (an annex or such), or a reference to existing policies and other documents that define security policies. A sole reference to a provision in the law does not fulfil this control. A specific agreement should describe in detail the procedures and measures for data security, namely the security service, antivirus systems, firewalls, etc.	Article 11(2) of the PDPA

Number	Control list	YES	NO	C	P	Guidelines how to fulfil the control	Legal reference
						Warning: a provider from a third country has to respect the security provisions of the PDPA, pay attention to the provisions on traceability of data processing[19].	
6	The contract with the service provider specifies the type(s) of processing activities and the provider's authorisations.	☐	☐	x	x	The contact (or an appropriate document as part of the contract) between the client and the cloud provider has to define precisely what types of data processing *may or has to be* executed by the provider – the scope of authorisations entrusted to the provider has to be clearly defined. The life cycle ensures data security from collection and use to destruction, and has the procedures and processes documented. Example: the client needs to know, whether the provider makes (also) back-up copies. In some cases it is necessary to also define what SHOULD NOT be executed by the provider (for example to make copies of data for its own purposes).	Article 11(2) of the PDPA
7	The client has to be informed at all times about any sub-processors, that may process its data on behalf of the cloud provider, and about the	☐	☐	x	x	To fulfil the requirement the provider may offer to its clients an updated and accessible list of all the subcontractors together with a description	Article 8 of the PDPA

[19] Traceability of data processing refers to the ability of subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

Number	Control list	YES	NO	C	P	Guidelines how to fulfil the control	Legal reference
	types of data processing they execute (transparency principle). The provider has to inform the client on any intended changes regarding the use of subcontractors in a reasonable timely fashion, so that the client has the time to decide whether it will terminate the contract due to the new subcontractor(s). Transfer of data to a subcontractor without the client's consent is inadmissible.					of their data processing activities. The subcontractors must ensure the same level of data security as the cloud providers – the transfer of data processing activities must not result in lowering of the level of personal data protection. In case the client and the provider disagree regarding a certain sub processor, the provider must offer the client enough time before termination of the contract, when the client can transfer back its data.	
8	After termination of the contract or at the request of the client, the provider must destroy all the personal data belonging to the client, including all back-up copies.	☐	☐	x	x	The client has to be informed when the personal data entrusted to the provider will be actually deleted and how. The providers that cannot inform the clients truthfully and fairly[20] about when and how the data will be deleted do not fulfil the requirement of this control. The client must be aware that it needs to retain usability of data even after termination of the contractual processing; that is why the provider has to enable the client to receive its data in such a structured electronic format, which	Article 21 of the PDPA

[20] Fairly refers to the obligation that important information is not withheld.

Number	Control list	YES	NO	C	P	Guidelines how to fulfil the control	Legal reference
						allows for further processing. The client must be aware that the data processing traceability logs are an integral part of the personal data.	
	Information security (security of personal data) – compliance and auditing						
9	Before using cloud services the client has conducted a risk analysis, alone or with a trusted third party.	☐	☐	x		In the risk analysis the data controller should consider proportionality in terms of the scope and sensitivity of the personal data being transferred to the cloud (see examples in the last chapter). We recommend that the risk analyses are conducted with the use of relevant methodologies such as the ISO/IEC 27005:2008, ENISA Cloud Computing Security Risk Assessment or other established standards.	Article 24 of the PDPA
10	Physical location of the personal data is known in every phase of the processing.	☐	☐	x	x	The client is informed about the location (exact address) of all the data centres, where any phase of the data processing will take place, and the locations of all sub-contractors processing the data. The provider has to offer the client true and fair information on the location and type of data processing (for example, it should not withhold the information on possible transfer of data to	Article 24 of the PDPA

Number	Control list	YES	NO	C	P	Guidelines how to fulfil the control	Legal reference
						third countries in a certain phase of processing). The client can for example request the provider to state that clearly.	
11	The client has a contractual right to audit the provider's information system or the audit of the whole information system is performed regularly by an independent third party. The provider informs the clients/publishes the results of the audits of the information system and security checks as provided by the law and security standards.	☐	☐	x	x	It is recommended that the provider conducts an independent audit of the whole information system at least once a year, comprising of IT management, security, and continuity of business, and to acquire an opinion from an independent auditor of information systems about all the controls of the audit. An internal audit by the provider does not fulfil the requirements of this control.	Article 11(2) of the PDPA
12	The provider encrypts the data transferred to or inside the cloud over unprotected communication networks.	☐	☐	x	x	Secure communication networks ensure confidentiality, authenticity and integrity of data. This is not the case with the transfer of data outside of the data client's control (for example over the internet) if during transfer the data are kept confidential and unchanged.	Article 24 of the PDPA
13	The client is informed about actual incidents[21] and on the policies regarding incident detection and management, including the mechanisms planned and described in the	☐	☐	x	x	Incidents must be regularly documented and handled. The procedures should be defined in advance and regularly updated. The provider's SLA[22] should provide for the necessary support	Article 24 of the PDPA

[21] Future legislation in the field of data protection will likely introduce mandatory data breach notifications (of the injured individuals and/or the competent authorities).
[22] Service Level Agreement

Number	Control list	YES	NO	C	P	Guidelines how to fulfil the control	Legal reference
	incident response action plan.					in handling the incidents, for an efficient execution of the incident response plan for every phase in the procedure: - detection - analysis - containment - eradication - recovery. Testing of the incident response plan should be executed at least once a year.	
14	The client needs to be informed about the approach used by the provider for resource sharing and with the technical and other measures used to address security aspects of multi-tenancy.	☐	☐	x	x	The client needs to know, whether it will be provided with its own physical or logical resources (with virtualization), and whether its data are separated from the data of other clients only logically and are stored in a common data base or a data carrier, etc. The clients should check whether their logical separation and multi-tenancy systems are acceptable in terms of legal requirements in their area. The clients should assess the risks, brought by multi-tenancy systems (logical separation, super administrators, isolation breaches etc.).	Article 24 of the PDPA

15	The provider protects its multi-tenancy infrastructure and informs the clients about security approaches.	☐	☐	x	x	The client should request from the provider a description of the security controls that protect the provider's multi-tenancy platform. The most important among the controls are: • Approaches used to separate different tenants in the information environment (for example separation with the VLAN network, processing/memory separation of virtual machines, application separation in SaaS applications, etc.). • Approaches for protection of the provider's multi-tenancy platform software against attacks. • Approaches used for strengthening and resilience of the providers infrastructure (such as hypervisor hardening, network devices, operation system, proprietary software) and for ensuring resistance to software errors, such as software updates procedures, testing and change management procedures, etc. Based on the above the client should assess additional risks raised by multi-tenancy and potentially introduce new controls.	

	Rights of an individual						
16	The client is satisfied that the providers' procedures and infrastructure enable easy access to personal data in case of a request from an individual to access his/her data, inside the deadlines provided by the law.	☐	☐	x	x	The client must be aware that it will have the obligation to facilitate exercise of data subjects' rights to access, correct or delete their data even if the data are in the cloud, where it will require the cloud provider's support. The processes and time frames regarding the exercise of individual's right to access the data processed in the cloud should be foreseen and defined in advance.	Articles 30 to 32 of the PDPA
	Transfer of data to third countries						
17	The client is informed about (all) the third countries the data will be transferred to.	☐	☐	x		Personal data will be stored and processed only in the EU/EEA area or Personal data will be transferred to third countries (outside EU/EEA).	Articles 63 - 71 of the PDPA
18	**Legal grounds for transfer of personal data to each of the third countries**					In case of transfer of data outside of the EU/EEA, the client must demonstrate legal grounds for such transfer (points 1 do 7)	
	1. The country where the cloud provider is based or where the data will be processed (even if only for a short while) is on **the list of the Commissioner**, and fully or partly ensures adequate level of data protection: Switzerland, Croatia, USA-Safe Harbor, Macedonia (**no prior**	☐	☐	x	x		Article 63(2) of the PDPA

	authorisation).						
	The cloud provider is certified as compliant with the Safe Harbor Principles and fulfils all the other control point requirements **(no prior authorisation).**	☐	☐	x	x		Article 63(3) of the PDPA
	2. The basis for transfer is one of the exemptions **(no prior authorisation is necessary,** even if the country does not ensure adequate level of protection): 2.1. provided by another statute or binding international treaty; 2.2. the individual gives consent and is aware of the consequences of such supply; 2.3. the transfer is necessary for the fulfilment of a contract between the individual to whom the personal data relate and the data controller, or for the implementation of pre-contractual measures adopted in response to the request of the individual to whom the personal data relate; 2.4. the transfer is necessary for the conclusion or implementation of a contract to the benefit of the individual to whom the personal data relate, concluded between the data controller and a third party; 2.5. the transfer is necessary in order to protect from serious danger the life or body of an individual to whom the personal data relate; 2.6. the transfer is performed from registers, public books or official records which are intended by statute to provide information to the public and which are available for consultation by the general public or to any person who demonstrates a legal interest	☐	☐	x	x	Only for transfers that are neither massive nor regular!	Article 63(3) of the PDPA, points 1 to 6

	that in the individual case the conditions provided by statute for consultation have been met;						
	4. The country where data will be processed **is on the list of the European Commission (prior authorisation needed!)**	☐	☐	x			Articles 63(1) and 67 of the PDPA
	5. **Standard contractual clauses** are concluded with the cloud provider **(prior authorisation needed!)**	☐	☐	x	x	Define the model: controller to controller / Controller to processor.	Article 70(1) of the PDPA, point 7
	6. The provider is bound by accepted **Binding Corporate Rules (prior authorisation needed!)**	☐	☐	x	x		Article 70(1) of the PDPA, point 7
	7. We concluded a **different type of a contract with the provider, so that adequate level of data protection is ensured** (see model clauses for example) **(prior authorisation needed!)**	☐	☐	x	x		Article 70(1) of the PDPA, point 7

5. EXAMPLES

To increase clarity, in this chapter we offer some real life examples that might be encountered by the data controllers interested in the cloud computing offers, or the cloud service providers wishing to be compliant with the legislation. The cases show how the guidelines may be of help in the decision making processes.

Case 1 – A small enterprise and office software suite in the cloud

A small enterprise wishes to process the data of their newsletter subscribers (natural and legal persons) using one of the popular office software packs in the cloud. The provider is certified as compliant with the Safe Harbor and has SSAE 16 type II certificate and thus claims to protect "privacy". With the use of the control list the enterprise comes to conclusion that it does not have the information on the exact location of their subscribers data, whether the data will be transferred to third countries (the terms of use provide that the data will be stored in the USA and in any other country where the provider has its facilities), how traceability of data processing is ensured, and when the data will be deleted from the provider's system. The terms of use are final and unchangeable. Because of the lack of information and transparency the small enterprise decides to review the offers of other providers and to assess the risks cloud processing might bring. If the data got lost or were disclosed publicly, the small enterprise would be held liable as a data controller.

Case 2 – Example of a data controller in the public sector

A primary school wishes to store and process the data on their pupils (including the e-grade book) with a cloud provider from the USA. The primary school is part of the public sector and has to, firstly, check whether there are legal grounds that allow for the data on their pupils to be processed (a law has to allow for such processing). With the use of the control list the primary school finds that the cloud provider's data centres, where the data will be stored, are in the USA and in India. The provider is certified under the Safe Harbor framework. It reserves the right to change the terms of service unilaterally anytime and hire new data centres for data storage. The primary school would be bound by the contract to use the services for two years, regardless of the changes. The service provider intends to use the data for its own purposes, to build statistics. All other requirements from the control list are fulfilled (regarding data security, audit, use of certificates, etc.). The primary school decides that the offer is not in line with a number of requirements from the control list and starts negotiations with the provider. At the end it achieves that the provider offers to sign standard contractual clauses for transfer of data to third countries, in addition to its Safe Harbor commitment. The contract as well provides that the primary school may terminate cooperation immediately and without any consequences if the terms of service change or another sub-contractor is enlisted by the provider. The provider must notify the school of any intended changes in such a timely fashion, that the school may choose another provider and move its data. The contract also states that the cloud provider MAY NOT use the data for its own purposes, not even to build statistics. Since all the requirements from the control list are met, the school may start processing its data in the cloud.

Case 3 – Enterprise level example

An enterprise wishes to transfer to a public cloud IaaS an information service that processes and stores personal data. The only open question is security of personal data during transfer over un-trusted networks. In the risk assessment the enterprise found that the risks occur during transfer of the data between the enterprise and the cloud and within internal transfers inside the cloud (transfer of virtual machines over the network, replication of the storage disks…). The enterprise requested information on security of transfers inside the multi-tenancy systems from all the potential providers, and then chose the one that encrypts all of the internal communications over un-trusted networks, in accordance with cryptographic policy of the enterprise (algorithms, length of keys, key management) and at the same time enables establishment of a secure VPN connection with the clients. Following the request, the cloud provider provided its security policy and a certificate on inclusion of the policy in regular ISO 27001 audits. The chosen provider had to assure in the contract the enterprise the right to audit the information system or to assure that independent external audits of the whole information system are performed regularly. Additionally, in the Service Level Agreement, the enterprise bound the provider to ensure legally appropriate level of personal data and sensitive data. The enterprise also checked, whether the provider has servers abroad (which may be considered as transfer of data to third countries) and if such transfer is legally admissible in their case.

Case 4 – Enterprise level example

A large enterprise already has its own information system and a new web service was introduced with the potential of a great number of new users. The management decided to host the service at an external provider, due to greater adaptability and lower initial costs. The enterprise already had a risk assessment made, however it had to adapt the assessment to the cloud environment. The enterprise found that the use of cloud services will directly impact on security of the existing information system, because the new service reads and writes data (including personal data) to it. The enterprise also found that its security policies and controls are not in line with the provider's. A gap analysis was carried out where the controls and other risk management measures in the enterprise and at the provider were benchmarked. After negotiation the service provider included additional controls in its policies and thus assured that the level of data protection will not be lowered by processing the data in the cloud and that production, test and development environments will be kept separate. The solution was initially part of a management assessment; however, before conclusion of the contract internal auditing department was included and a certified information systems auditor took part at every stage of the project (conclusion of the contract, development, testing, and launch of the service).

Case 5 – A small enterprise and the use of a cloud based customer relationship management (CRM) solution

A company wishes to implement a solution for customer relationship management in the cloud. A local provider provides the service in cooperation with a partner from abroad – the data are stored at different locations, mostly outside the EU. After reviewing the offer the enterprise finds that the provider DOES NOT define exact physical locations of the servers, where data would be placed. In the offer there is also no provision regarding handling of the data after termination of the contract. The enterprise informs the provider and negotiates that the new contract includes specifically defined locations of the infrastructure and a detailed security policy. The contract also addresses handling of data in the event of contract termination where the provider is instructed to physically destroy all the data, including back-up copies in a certain timeframe. The local provider also fulfils the requirements of all other controls from the list, especially related to transfer of data to the foreign partner's servers in countries outside the EU.

Case 6 – A local provider of cloud services

A cloud service provider (office software suite and internet communication tools) is a local provider, renting data facilities in Brazil, Mexico and India. It intends to offer its services to SMEs in Slovenia. The provider offers a standard contract, where it reserves the right to enlist new sub-processors in or outside the EU at any time and does not offer the clients access to the full list of sub-contractors. The contract does not include provisions on data breach detection or handling, nor it includes an incident management plan. It addresses security procedures and measures only by a reference to a provision in the law. There is no information regarding security of its multi-tenancy infrastructure. The provider soon finds the requirements of the legislation, with the use of the control list, and adapts its practices and transparency. It also finds that it is responsible for adequate security of the data it is entrusted with, and that in the case of non-compliance, it may be held liable in the course of an inspection or offence procedure which may result in sanctions.

6. CONCLUSION

Considering all the above, the Commissioner recommends that the data controllers conduct a **proper risk analysis** before moving their data to the "cloud" and that sensitive data, such as medical data and data with a higher degree of sensitivity, are not transferred to the cloud before stronger safeguards are implemented. It should be remembered that the data controller is primarily the one, bearing responsibility for any abuse of the personal data; that is why it has to be strongly convinced that the contractual providers and their sub-providers are able to offer appropriate guaranties. The Commissioner especially emphasises that in the case of providers from the USA their sole certification under the Safe Harbor framework does not mean that all the requirements regarding data security and contractual data processing from the PDPA are fulfilled; even though there is no requirement to ask the Commissioner for approval of the transfer. Any service provider that is unable to provide adequate information and assurances regarding security of the data, should be regarded with a degree of precaution and restraint by clients who are able to correctly assess the risks connected to the processing of their data. The client or the data controller is in the end the one that has to assess the risks and decide whether a certain cloud provider can be trusted, and the client will be held liable for its decisions.

In the end the Commissioner offers general recommendations regarding cloud computing. The Commissioner believes that:

- cloud computing raises vast potential, however this should not lead to lowering of the level of personal data protection, a fundamental human right;
- further efforts need to be put in research, standardization and certification schemes, and in adaptations of the legal and regulatory frameworks for raising the level of trust in cloud computing services;
- the data controllers must conduct proper risk assessments and privacy impact assessments before the use of cloud computing, if needed with the assistance of trusted third parties;
- cloud providers must improve their transparency towards the clients, foremost regarding information security assurances;
- supervisory authorities in the area of data protection and privacy protection must continue with developing guidelines and raising awareness regarding data protection and privacy issues.

7. USEFUL SOURCES AND LINKS

- Cloud Computing: Benefits, Risks and Recommendations for Information Security. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

- CSA Security Guidance v.3, CSA Cloud Controls Matrix, CSA Consensus Assessments Initiative: https://cloudsecurityalliance.org/research/.

- Article 29 Working Party opinions. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

- ENISA Cloud Computing Information Assurance Framework. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.

- ENISA Security and Resilience in Governmental Clouds (2011). http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

- ENISA Procure Secure: A guide to monitoring of security service levels in cloud contracts. http://www.enisa.europa.eu/activities/application-security/test/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts.

- IWGDPT: Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland): http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

- NIST Definition of Cloud Computing - NIST SP 800-145. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

- NIST Cloud Computing Synopsis and Recommendations - NIST SP 800-146. http://csrc.nist.gov/publications/nistpubs/800-146/SP800-146.pdf.

- INDUSTRY RECOMMENDATIONS TO VICE PRESIDENT NEELIE KROES ON THE ORIENTATION OF A EUROPEAN CLOUD COMPUTING STRATEGY - November 2011 http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7672&utm_campaign=isp&utm_medium=rss&utm_source=newsroom&utm_content=tpa-261.