International Working Group
on Data Protection
in Telecommunications

675.44.8 24 April 2012

Working Paper
on

Cloud Computing - Privacy and data protection issues

- "Sopot Memorandum" -

51st meeting, 23-24 April 2012, Sopot (Poland)

Scope

This working paper specifically examines the processing of personal data in cloud computing environments.

The working paper does not examine a situation in which all end users, the controller, the processor and all of its subcontractors are subject to the same data protection legislation and are physically located within the same jurisdiction and all data processing and data storage takes place within this jurisdiction. This paper is also of less relevance, where the cloud service is totally under the control of the cloud service user.

Finally, the working paper only deals with the use of cloud services by companies and public authorities which move existing procedures "into the cloud", not with the use of such services by individuals.

General Background

> *"Cloud computing is an evolving paradigm."* [1]

Cloud Computing (CC) is attracting increasing interest due to promises of greater economic efficiency, lower environmental impact, simpler operation, increased user-friendliness and a number of other benefits.

In September 2011, the National Institute of Standards and Technology (NIST) released Special Publication SP 800-145, in which it defined cloud computing as:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."* [2]

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The definition is, among other things,

> *"..... intended ..... to provide a baseline for discussion from what is cloud computing to how to best use cloud computing."* [3]

The definition is an important contribution to the ongoing process of understanding what CC actually is. This understanding is developing rapidly. The NIST definition is an excellent starting point for further investigation of CC and how to use it.

However, there is still uncertainty in relation to CC, especially when it concerns privacy, data protection and other legal issues. The recommendations in this paper are intended to help reduce that uncertainty.

The paper is structured to present the recommendations first. The second part of the paper provides additional background on cloud computing as well as the rationale behind the recommendations. For deeper insight, readers might benefit from reading this section first.

For the purposes of this paper, the cloud customer is deemed to be the data controller and the cloud service provider is deemed to be the data processor.[4]

The evolution of CC has highlighted a number of important issues, including:

a. there is not yet international agreement on common terminology;
b. the development of the technology is still in progress;
c. enormous amounts of data are being accumulated and concentrated;
d. the technology is boundless and transboundary[5];
e. data processing has become global;
f. transparency is lacking with respect to cloud service provider processes, procedures and practices, including whether or not cloud service providers sub-contract any of the processing and if so, what their respective processes, procedures and practices are;
g. this lack of transparency makes it difficult to conduct a proper risk assessment;
h. this lack of transparency also makes it more difficult to enforce rules regarding data protection;
i. cloud service providers are under great pressure to quickly capitalise significant investment costs;
j. cloud customers are under increasing pressure to reduce costs, including those of their data processing, in part accelerated due to the global financial crisis; and
k. to keep low prices cloud service providers are more likely to offer standard terms and conditions.

These circumstances may lead to **an increased risk of**:

A. breaches of information security such as breaches of confidentiality, integrity or availability of (personal) data unnoticed by the controller;
B. data being transferred to jurisdictions that do not provide adequate data protection;
C. acts in violation of laws and principles for privacy and data protection;
D. the controller accepting standard terms and conditions that give the cloud service provider too much leeway, including the possibility that the cloud service provider may process data in a way that contradicts the controller's instructions;
E. cloud service providers or their subcontractors using the controllers' data for their own purposes without the controllers' knowledge or permission;
F. accountability and responsibility seemingly fading or disappearing in a chain of subcontractors;

G. the controller losing control of the data and data processing;
H. the controller or its trusted third party (e.g. auditor) being unable to properly monitor the cloud service provider;
I. data protection authorities being precluded from properly supervising the processing of personal data by the controller and the cloud service provider; and
J. the controller relying on unfounded trust in the absence of insight and monitoring, thereby potentially contravening the data protection legislation in force in the country of establishment.

The following recommendations are intended to help **reduce risks associated with the use of cloud computing services and to promote accountability and proper governance**[6], so that the benefits of utilising CC can be achieved, but not at the expense of the rights of the individual.

Recommendations[7]

General recommendations

The Working Group recommends that:

- Cloud computing must not lead to a lowering of data protection standards as compared with conventional data processing;
- Data controllers carry out the necessary privacy impact and risk assessments (if necessary, by using trusted third parties) prior to embarking on CC projects;
- Cloud service providers further develop their practices in order to offer greater transparency, security, accountability and trust in CC solutions in particular regarding information on potential data breaches and more balanced contractual clauses to promote data portability and data control by cloud users;
- Further efforts be put into research, third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in CC;
- Legislators reassess the adequacy of existing legal frameworks allowing cross-border transfer of data and consider additional necessary privacy safeguards in the era of CC[8], and
- Privacy and Data Protection Authorities continue to provide information to data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues.

Additional guidance on best practices

1. CC implementation should take place in careful, measured steps, starting with non-sensitive and non-confidential information.

2. The processing of sensitive[9] data via CC raises additional concerns. Therefore without prejudice to national laws such processing requires additional safeguards.

3. **Location audit trails** should be made available to controllers and DPAs. The audit trail should be recorded automatically and show the physical locations in which personal data have been stored or processed and when[10].

4. **An automatically rec**orded **copying and deletion audit trail** should be established, showing clearly which copies of personal data the processor or its subcontractors have created and deleted.

5. The location audit trail and the copying and deletion audit trails should also include backup.

6. Effective **technical measures** should be developed against personal data illegally being transferred to jurisdictions without sufficient data protection.

7. It should be ensured that **deletion** of personal data from disks and other storage media can be executed in an effective way, e.g. through **immediate overwriting with random data**[11].

8. It should be ensured that personal data at rest and in transit[12] are **encrypted** using recognised standard algorithms and contemporary key lengths. The encryption keys should not be used by, or be accessible to anyone others than the controller and cloud service provider. The encryption keys should not be used by, or be accessible to other customers of the cloud service provider. Data should not be available in unencrypted form longer and more extensively than is absolutely necessary for the data processing process at hand. Methods rendering data unreadable to CC providers at any given time should be further explored[13]. It could be useful to explore options by which the controller can effectively and quickly cut off the cloud service provider or its subcontractors from decrypting data (an emergency brake).

9. There should be automatic **logging** of all uses of personal data by cloud providers and their subcontractors. The log should be easily accessible to the controller and be designed in a simple, readily understandable form. The cloud service provider and its subcontractors should ensure the integrity of the logs.

Controller

10. In the agreement with the cloud service provider, the controller should secure a complete list of information in advance about all physical locations in which, throughout the duration of the agreement, data may be stored or processed by the cloud service provider and/or its subcontractors, including backup (**principle of location transparency)**.

11. In the agreement, the controller should ensure that neither the cloud service provider nor its subcontractors transfer data to locations other than the physical locations listed in the contract, regardless of their reason for so doing, and regardless of whether the data are encrypted. This should be supported by technical measures whose existence and dependability the controller has an actual ability to inspect.

12. The controller should ensure that the agreement with the cloud service provider does not contain ambiguities or room for interpretations which undermine the principle that the cloud service provider only processes personal data according to the controller’s instructions. Should cloud service providers be able to unilaterally change the agreement the controller should have the right to terminate the contract and to transfer the data to a different cloud service provider.

13. The agreement should explicitly state that the cloud service provider may not use the controller’s data for the cloud service provider's own purposes.

14. The controller should have the opportunity to inspect or have inspected all locations that process personal data wholly or partially in the present or have done so in the past, or may do so in the future under the agreement. The agreement should specify that the controller has the right to obtain full insight into all aspects of the cloud service provider and its subcontractors that the controller deems necessary to ensure compliance with the agreement, including ensuring that processing of personal data is done according to instructions, is done legally and in a suitably secure manner.

15. In the agreement, the controller should secure the right to let a trusted third party (e.g., a recognized auditing firm)[14] wholly or partially monitor the processing of personal data by the cloud service provider and its subcontractors, if any.

16. Prior to the use of CC, the controller should perform a **risk assessment** based on insight into the specific conditions and circumstances under which personal data will be processed by the cloud service provider and its subcontractors, if any. The risk assessment should include all of the locations at which personal data are processed or stored. If the cloud service provider uses subcontractors for parts of the processing, the risk assessment should also include all locations used by the subcontractors.

17. The controller should regularly review and update the risk assessment as long as personal data are processed by the cloud service provider.

18. Before use of CC, the controller should consider ensuring that there is a real exit option with the cloud service provider, including an active role in the transfer of data by the cloud service provider, in order not to become dependent on the cloud service provider (lock-in).

19. The controller should consider whether it is necessary to secure access to at least one usable copy of data outside of the cloud service provider's (and its subcontractors') control, reach or influence. If this is deemed necessary, the copy should be accessible and usable by the controller independently of the cloud service provider's and its subcontractors' participation.

20. The controller should be able to fully fulfil its obligations towards data subjects and Data Protection Authorities in case of a **data breach** and take appropriate actions accordingly. As such, the controller should make clear agreements with the cloud service provider regarding a prompt and complete notification of the controller and/or Data Protection Authority in case of such a data breach.

21. The controller should contractually oblige the cloud service provider to implement effective and prompt procedures so that the data subjects can exercise their rights of access, rectification, erasure or blocking of data.

Cloud service provider

22. The cloud service provider should establish full transparency for the controller regarding the locations used for data processing and storage of personal data by the cloud service provider and its subcontractors, if any.

23. The cloud service provider should establish full transparency regarding the subcontractors used and what processing they perform for the cloud service provider.

24. The cloud service provider should provide transparency in contractual matters and refrain from offering CC on standard terms and conditions that allow for unilateral contract changes.

25. Cloud service provider and their subcontractors, if any, are encouraged to follow best practice and allow an impartial third party to conduct a comparison and assessment thereof (benchmarking).

26. Standard terms and conditions offered to certain market segments, e.g. small and medium enterprises should be drafted in such a way that respect of privacy and appropriate safeguards are taken into account.

Auditing

27. Given the possibility of very large accumulations of personal data by the cloud service provider, the cloud service provider should be subject to third-party audits in addition to the audit performed by the controller in the controller's own interest. The auditor should be fully independent of the cloud service provider and should pay special attention to the security aspects of processing of personal data. In particular, the auditor should check whether measures regarding the following are in place and functioning properly: location audit trail (see section 3), copying and deletion audit trails (see section 4), deletion (see section 7), and logging (see section 9). Further, the auditor should check that the following are in place and functioning properly: measures to prevent the illegal transmission of data to jurisdictions with insufficient data protection (see section 6) and measures to prevent the transmission of data to other locations than those explicitly agreed with the customer (see sections 10 and 11). Lastly, the auditor should ensure that it is not possible for the cloud service provider or its subcontractors, if any, to circumvent these measures undetected.

Background for the recommendations

28. CC is a relatively **new paradigm** for data processing, evolving from what, for lack of a better term, is now being referred to as **traditional data processing**. Many years of solid experience with traditional data processing have accumulated, whereas there is no similar solid experience with CC.

29. The consequence of the **paradigm shift** is that basic assumptions, experiences, ideas, theories and models for data processing no longer correspond to the practice, and therefore must be subjected to critical reflection, reassessment and possible revision. This also applies to privacy and data protection of personal data and how **risks** can be analysed, assessed and judged. What was best practice yesterday is not necessarily best practice today.

30. The **new situation** must be examined and implemented with **carefully measured steps**, particularly with regard to privacy and data protection, and protection of the rights of the data subject in a wider sense.

31. The **technical foundation** of CC is well-developed network technology and virtualisation of servers. This enables quick dynamic relocation of data and data processing among servers locally in the individual cloud data centre and globally among cloud data centres in countries around the world. The technology is highly scalable without creating limiting bottlenecks. The internet allows the end user to access the data regardless of where the cloud data centres are located.

32. The **economic driving force** behind CC is **economics of scale**. Consolidating data processing in large centres improves the utilisation of expensive resources such as: human knowledge, tangible capital (HW, SW, buildings), communication bandwidth and energy. In addition, due to their size and volume, cloud service providers have significant bargaining power when purchasing resources. Cloud service providers can therefore reduce unit costs and offer attractive prices to customers. The prerequisite for achieving economics of scale is

many customers in “the store”. To achieve sufficient **volume**, CC services are offered globally via the internet.

33. CC is considered to provide important opportunities for small and medium enterprises to have access to affordable and scalable computing resources. Due to the large number of relatively small entities, it is expected that cloud service providers will develop standard terms and conditions for this market segment.

34. CC is far more dynamic than traditional data processing. The location where data processing takes place can change dramatically. The current location of data and where it is processed can depend on a variety of factors to which end users and data controllers traditionally have given little thought, and into which they do not necessarily have the insight or ability to control. For example, cloud service providers often choose to locate their data centres across many countries and several continents, based on the availability of cheap electricity, a cool local climate and time zone differences, among other factors. Unpredictable circumstances can also impact the current location of data, such as interruptions in one data centre or a lack of capacity at peak periods (overflow). Copies of data can be transferred to other data centres to ensure online accessibility in case of interruptions in one data centre or for the purpose of making backups (redundancy).

35. CC is based on many cloud customers dynamically sharing a common pool of the cloud service provider's resources. This should only take place if it is possible to maintain **robust separation** of the different cloud customers’ data and their processing. Resource sharing entails an increased risk of large scale losses or unauthorised disclosure of data.[15] The risk is further enhanced by the fact that CC is driven by cost optimisation based on high volume (economics of scale). Cloud customers constitute a risk to each other. The more customers sharing the same resources, the greater the risk for each individual customer, and thus for cloud customers as a whole.

36. Knowledge about CC and insight into its risks are currently concentrated among relatively few large cloud service providers, who for commercial and competitive reasons appear to be reluctant to give the world insight into specific conditions and circumstances. The uneven distribution of knowledge and insight between cloud service providers and customers places the latter in a weak position when entering into agreements and makes it difficult for them to properly assess risks associated with the intended use of CC.

37. A thorough **risk assessment** must be based on **insight** into the concrete setup and circumstances of the cloud service provides at all of the locations where data processing will take place.

38. CC technology is **boundless** and **transboundary**. The global customer base, in tandem with the global distribution of cloud data centres and dynamic movement of data (and data processing), can result in data crossing national borders and changing jurisdictions with a corresponding lack of transparency. Personal data may end up in data centres in jurisdictions with inadequate data protection or personal data may be misused commercially or be accessed without authorisation by foreign powers[16].

39. A distinction must be made between the two mutually exclusive roles of controller and processor within data protection. The **controller** is the one who determines the purpose and means used for a specific act of data processing.

40. It is also widely acknowledged that a controller may allow the processing of personal data to be performed by a **processor** but only in accordance with the controller’s explicit **instructions**.

41. A commonly recognised data protection principle is that the processor must not process personal data to a greater extent than that which follows from the explicit instructions from the controller.[17] For CC, this implies that a cloud service provider cannot unilaterally make a decision or arrange for personal data (and its processing) to be transmitted more or less automatically to unknown cloud data centres. This is true whether the cloud service provider justifies such a transfer as a reduction of operating costs, management of peak loads (overflow), load balancing, copying to backup, etc. Nor may the cloud service provider use personal data for his own purposes.[18]

42. Another generally recognised data protection principle requires that the controller implement appropriate **technical and organisational security measures** to protect data against accidental or unlawful destruction, loss or deterioration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down by the law. The same applies for processors.

43. Fulfilment of the controller's responsibility requires that the controller **monitor** the processing by the processor to ensure that it takes place according to the controller's instructions and that the processing is done with adequate security.

44. Without removing his liability, the controller can give explicit instructions that monitoring of processing by the processor be partially performed by a **trusted third party** (e.g. auditor). The prerequisite is that the third party has the necessary qualifications, is independent of the processor, has full access to and insight into the actual conditions and circumstances under which processing by the processor takes place and can reliably report his observations, assessments and conclusions to the controller.

The Working Group will continue to monitor developments in the area of cloud computing and update this paper as necessary.

Notes

[1] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Page 2.
[2] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Page 3.
[3] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Page 2.
[4] Cf. paras. 39 and 40 below. The cloud service provider's subcontractors in connection with the processing of personal data are also considered processors.
[5] Cf. para. 38.
[6] On pages 9-10 of *Cloud Computing – Benefits, risks and recommendations for information security, November 2009*, ENISA lists the top security risks, in random order, as: loss of governance, lock-in, isolation failure, data protection, insecure or incomplete data deletion, malicious insider. For details see the publication. Loss of governance is emphasised here.
[7] The list of recommendations is not exhaustive.
[8] Cf. International Conference of Data Protection and Privacy Commissioners: International Standards on the Protection of Personal Data and Privacy ("Madrid Resolution"), 5th November 2009; http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf
[9] The concept of sensitive data carries different meanings in different legal cultures, cf. Art. 8 of Directive 95/46/EC, Art. 9 EU Draft General Data Protection Regulation and the FTC Report "Protecting Consumer Privacy in an Era of Rapid Change" (2012)
[10] E.g. the location audit trail could provide a clear overview of when the individual personal data are checked in and checked out at the individual locations, as well as when and to which location they are transferred.
[11] Deletion by dereference of data and later overwriting by reuse of the storage areas is generally not sufficient, as it opens the possibility that data become accessible again by renewed reference before or during the reuse of the storage areas.
[12] For data in transit end-to-end encryption should be applied. It must be ensured that personal data in transit is protected against active (e.g. replays, traffic injection) and passive attacks (e.g. eavesdropping). Furthermore, access to data in rest by unauthorised parties must be prevented via corresponding technical and organizational mechanisms (e.g., access control, encryption of the data).
[13] An example of research in this area is the Sealed Cloud initiative, which is presented in the preprint paper Sealed Cloud - a novel approach to defend insider attacks by Hubert A. Jäger and Arnold Monitzer. The preprint is available from http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf
[14] For more on trusted third parties, refer to section 44.
[15] On pages 9-10 of *Cloud Computing – Benefits, risks and recommendations for information security, November 2009*, ENISA lists the top security risks, in random order, as: loss of governance, lock-in, isolation failure, data protection, insecure or incomplete data deletion and malicious insider. For further details, refer to the publication; here it should be emphasised that isolation failure is considered a top risk.
[16] Whilst personal data may be processed within one jurisdiction, the cloud provider, or parent company, may also be established within another jurisdiction thereby allowing foreign law enforcement powers access to the data within the cloud service even though that data physically resides outside the geographical boundaries of that country. An international agreement may be required to address this issue.
[17] Or by legislation.
[18] If cloud service providers process data without the knowledge of the controller, the cloud service provider should be seen as a co-controller and as such be held accountable for the unauthorised independent processing of data.