CLOUD
ACCOUNTABILITY
PROJECT

Brokering Cloud Offerings based on Data Protection Requirements

Project Release

This document has been edited by Rehab Alnemr (HPE).

Contributors to this document include Rehab Alnemr (HPE), Siani Pearson (HPE), Dimitra Stefanatou (Tilburg University), Lorenzo Dalla Corte (Tilburg University), Asma Vranaki (QMUL), Niamh Gleeson (QMUL), Amy Holcroft (HPE).

This work has been partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no:317550 (A4CLOUD) Cloud Accountability Project.

Brokering cloud offers

There are an abundance of cloud offerings that differ in their properties such as price, bandwidth, availability, security, etc. Cloud brokers connect cloud customers with suitable providers based on these properties. Functionalities of a cloud broker typically include consolidated billing, seamless switching between providers, matching services with customer requirements and monitoring.

What is the value of cloud brokerage?

Customers have access to a vast quantity of product and pricing information online. This wealth of information sometimes threatens to overwhelm them and complicates decision-making. Cloud brokers, especially online cloud brokerage tools, provide a useful and quick way to help decision-making by comparing various offers and, in some cases, finding the most suitable deal for the individual customer.

What is missing in cloud brokerage?

Among other things, matching the contract terms in cloud providers' service offerings with the user's non-functional requirements -- such as transparency, legal terms, court of choice, privacy and security, etc and on the basis of data protection requirements. Some of these non-functional requirements are mentioned in the contracts but they are not clearly categorised nor used in offers-requirements matching. This leaves some offers with a less transparent description.

Our approach: the identification of the relevant attributes

We have created a list of attributes - relating to data protection- that can be used when matching cloud offerings with user requirements. This list is based on the analysis of standardised cloud contracts, service level agreements (SLAs), the EU Data Protection Directive (DPD)[1], and the EU Data Protection Regulation (GPDR)[2] as well as academic literature. The analysis resulted in identification of 16 attributes that can be used to filter and match offers aiming, ultimately, at enabling the user making an informed choice from the viewpoint of personal data protection.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L281/31 (DPD) (1995)

[2] COM 11 final 2012/0011 (COD) European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, 25.1.2012 p. 1. (2012)

Attribute categories

1. **Security measures**: encryption of data in transit and at rest and the management of the encryption keys
2. **Locations**: will be one of the criteria to determine which data protection and privacy laws apply
3. **Data protection roles**: whether the cloud service provider (CSP) is acting as a data controller or processor as determined under EU law
4. **Data deletion**: if the CSP provides for specific deletion procedures
5. **Notification of changes of terms &conditions:** the process in which the CSP notifies its customer when it changes its terms of service
6. **3rd parties supporting the services**: the privacy and security related contractual terms of the cloud service a customer is using may be less effective if the cloud service subcontracts with third parties that have lower privacy and security requirements
7. **Reporting for incidents and security breaches**: the CSP notification of breaches to the cloud customer
8. **Notification of disclosure to law enforcement agencies (LEAs)**: whether the CSP informs the customer that law enforcement agencies requested his data
9. **Certification:** whether the CSP is certified in regular intervals
10. **Data retention after termination**: what happens to a customer's data after the termination of a contract
11. **Monitoring by the CSP:** whether the CSP monitors what happens to their service and in doing so, monitors customers' data
12. **Data portability**: can the customer move his data from one CSP to the other easily and seamlessly
13. **Business continuity plan**: whether the CSP provides for a business discontinuity plan in case of force majeure or corporate changes
14. **Dispute resolution**: whether any disputes can be resolved in the customer's own country
15. **Liability**: an indicator of a CSP adhering to high privacy and security requirements is whether or not it is prepared to incur liability for breaches of privacy and security
16. **Jurisdiction**: the location of the court where any dispute should be resolved will determine the jurisdiction

How can you use these attributes?

These attributes will guide you in setting your own requirements in order to best address your data protection and security needs by performing a comparative analysis of cloud service providers. They are presented in the form of an overall subject area associated with one or more questions designed to help identify the data privacy and security issues that are important for your business or for your personal life when selecting a cloud service provider. These attributes can be used as a guideline for those who want to create other brokerage tools covering data protection aspects. They are also a useful benchmark to take into account when defining cloud contracts.

List of Attributes

ID	Attribute	Explanation
Security Measures		
1	Do you want the CSP to encrypt your data?	Encryption is a mechanism by which data is transformed in a form that preserves confidentiality. Encrypted data remains unreadable to people who don't possess the decryption key. Encryption of personal data, in particular, is considered to be good security policy and best practice methodologies for protecting personal data.
2	Do you require the CSP to encrypt your data while at rest? and which kind of encryption? (OpenPGP, 256bit SSL, SSL, 2048-bit Encryption, OTR, RSA, Truecrypt, Client-side Encryption, Provider-Side Encryption, Hashing, Symmetric methods, Asymmetric methods)	Encryption of data at rest refers to data during the time it is stored within a CSP's systems. Encryption of data in transit refers to data during its transmission from your device/system to the CSP's system.
3	Do you require the CSP to encrypt your data while in transit? Which kind of encryption?	To establish stronger security, encryption of data at rest has to be combined with the encryption of data while in transit.
4	Which key management solution would be suitable for you needs? • key management functions performed by the cloud provider • key management functions performed by the customer • key management functions performed by a third party cloud provider • split key encryption and homomorphic key management	Encryption should be considered for both data in transit and at rest to protect it from unauthorised disclosure. The encryption key must be adequately protected as it is needed to convert data in its original form. If the key is lost data become useless and could amount to destroying personal data. If an unauthorized person comes into possession of the key, he can access personal and confidential data. The encryption key must be managed through a proper process.

ID	Attribute	Explanation
Processing Locations		
5	Where do you want your data to be processed? • Only in EEA/EU • USA • Third countries outside EEA/EU which provide an adequate level of protection	This question is particularly relevant when personal data are being processed. Personal data are data from which a living individual may be identified. Processing of personal data refers to any operation or set of operations which is performed upon personal data, such as collection, recording, storage, retrieval, consultation, use, erasure or destruction. EEA (European Economic Area) covers all member states of the EU plus Norway, Liechtenstein and Iceland. Third countries outside the EEA/EU which provide an adequate level of protection for personal data are those whose laws have been found adequate by the European Commission. These countries are Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States (Safe Harbour), Eastern Republic of Uruguay. If the CSP commits to only process data in a particular country, they are bound to keep data only within the indicated processing locations.

ID	Attribute	Explanation
Data Protection Roles		
6	In what capacity do you want the CSP to act in relation to your personal data? • As a data processor • As a data controller	Personal data is any data from which a living individual can be identified. A data processor is a CSP which processes personal data under your instruction and does not use the data for its own purposes. A data controller is a CSP which determines what your data is processed for and how it i0097s processed. The majority of CSPs opt for the role of data processors. This means you, the cloud customer, are liable for the processing of personal data in accordance with applicable law as the data controller. Data protection roles are not relevant if no personal data is being processed.
Data Deletion		
7	Taking into account the nature of the data you want to upload, do you want the CSP to provide specific data deletion procedures for data during the terms of the contract? (Data is deleted irretrievably, data are not archived or inactivated, or it does not matter)	The inclusion of contractual clauses ensuring specific deletion procedures guarantees that your data cannot be accessed by anybody else either by mistake or for malicious purposes. Only the CSP can offer secure deletion of data.

ID	Attribute	Explanation
Notification of changes of T&Cs		
8	Do you want to be notified of changes in Terms and Conditions?	Most CSPs reserve the right to unilaterally modify their terms of service. Some CSPs do not notify customers of changes directly, instead they post changes on the website. Others notify the customer by email. Minor changes are usually effective immediately, after posting on the website or sending the email. Several CSPs give advance notice for material changes to the terms and conditions, usually between 14-30 days. The majority of CSPs state that continued use of the services after notification indicates acceptance of these changes. A few CSPs offer the customer the right to terminate when notified of material changes in the contract.
Third parties supporting the services		
9	Do you want to allow the CSP to subcontract the services to third parties?	Third parties are companies or individuals used by the CSP to deliver all or part of the services.

ID	Attribute	Explanation
Reporting of incidents and security breaches		
10	Do you want to be notified in the event of a security breach involving your data?	In some jurisdictions the CSP will be under a legal obligation to notify you that there has unauthorized access or unlawful transfer of your personal data in certain circumstances. If a CSP agrees to notify you of security breaches it is likely to be limited to material breaches of security affecting your data.
Notification of disclosure to LEAs		
11	Do you want to be notified if a law enforcement agency requests to access your data from the CSP (if legally possible)?	Law enforcement agencies (LEAs) may request data from CSP's to help them investigate crimes. This is normally done on the basis of a warrant or court order. CSP's will often be prohibited from informing customers that they have received an LEA request. If it is possible to be notified that an LEA request has been made for your data, you will be able to object to the request if you believe that your data should not be disclosed.

ID	Attribute	Explanation
Certification		
12	Against which of the following controls would you require the CSP to be certified periodically, if any? 1. Information security policy 2. Risk management 3. Security roles 4. Security in Supplier relationships 5. Background checks 6. Security knowledge and training 7. Personnel changes 8. Physical and environmental security 9. Security of supporting utilities 10. Access control to network and information systems 11. Integrity of network and information systems 12. Operating procedures 13. Change management 14. I am not interested in any controls.	

ID	Attribute	Explanation
Data retention after termination		
13	Do you want the CSP to keep your data for a specific period of time following service termination?	If a CSP retains your data for a period after termination of the service, this may allow you to easily resume using the service if you change your mind. Alternatively you may want to ensure your data is deleted as soon as possible upon service termination or shortly thereafter.
Monitoring by the CSP		
14	CSP's often reserve the right to monitor your activities, for different purposes and with a different level of granularity. Which of the following options do you want to accept? • I want to use a CSP that does not monitor the information I entrust it. • I accept the CSP monitoring the content of the information I entrust it. • I accept the CSP monitoring the metadata of the information I entrust it, but not its content. • It does not matter	In principle, CSPs monitor to a certain extent the activities of their customers in order to be able to provide their services and secure their systems. The extent to which A CSP monitors data varies from provider to provider. A CSP may monitor (i)your activity (e.g. to verify whether you comply with their Service Level Agreement); and/or (ii)metadata of the information you entrust them (e.g the information about the information) and /or (iii) the actual content of the information you upload.

ID	Attribute	Explanation
Data Portability		
15	Do you want the CSP to allow for the portability of your data? • Yes a. Through a standard format (such as xml, JSON) b. Through a non-standard but documented format c. By providing support to export data after service termination • No • It does not matter	Data Portability is the ability to transfer your data from one cloud service to another and it is particularly relevant if you are likely to switch providers in the future. Data portability enables the re-use of data and can be achieved if the CSP you are leaving provides a mechanism to export your data and the CSP you are joining provides methods to import data. Data portability is a major concern for customers of SaaS cloud services as schemas and formats of data are under the control of the cloud provider.
Business Continuity plan		
16	Do you want the CSP to provide a business continuity solution?	The CSP may be unable to provide the service due to a series of factors or unforeseen events outside its e.g. electrical outage or bankruptcy. Some CSPs offer business continuity to ensure minimal disruption to your continued use of the service.

ID	Attribute	Explanation
Dispute resolution		
17	Is it important that any disputes with the CSP are resolved in your own country?	Disputes with a CSP may be resolved through arbitration, litigation, mediation, and court legal action or online. If you are a business, you need to decide whether you want to resolve disputes with your CSP in the country in which you operate or would be happy to do so in another country. A CSP will often require disputes to be resolved in its own country of establishment. Dispute resolution abroad may be more costly and time-consuming for you than in your own country so you should take legal advice on what the implications may be for you in accepting dispute resolution abroad.
Liability		
18	To what extent will you accept the CSP limiting its liability to you? • Entirely • Partly • It does not matter	Liability means taking legal responsibility for certain events and it is possible for a CSP to limit its liability for certain types of loss or put a limit or cap on the amount of money a customer can recover from it. Many CSPs will exclude all liability to customers except for those it cannot exclude by law e.g. fraud, death and personal injury caused by negligence. Other CSPs may partially limit their liability by excluding certain types of losses, typically indirect losses, consequential or economic losses arising from a breach by the CSP.

ID	Attribute	Explanation
Jurisdiction		
19	Where do you want the court to be located? • Own EU Member State • Other EU Member State • US Court • It does not matter	The large majority of CSPs are located in the US and will require court action to be brought in the USA. Court action in the USA may be more costly and time-consuming for you than in your own country so you should take legal advice on what the implications may be for you in accepting this. If you require court actions to be brought in the EU member state where you are located or another EU member state, this will limit your choice of cloud providers due to the predominance of US CSPs in the current cloud market.

Further information

- EU Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data (General Data Protection Regulation), 2012.
- Rehab Alnemr, Siani Pearson, Ronald Leenes and Rodney Mhungu ,“COAT: Cloud Offerings Advisory Tool”, In CloudCom IEEE Proceedings, 2014.
- A4Cloud Deliverable. D: D-4.3 Guidelines and tools for cloud contracts.

Contributors

Hewlett Packard Enterprise

Tilburg University

Queen Mary University of London

This research was carried out within the context of the EU FP7 Cloud Accountability Project (A4Cloud). This project is developing methods and tools, through which cloud stakeholders can be made accountable for the privacy and confidentiality of information held in the cloud.

For more information

- EU Cloud Accountability (A4Cloud) Project: http://www.a4cloud.eu
- info@a4cloud.eu