Checklist for Cloud Service Contracts

Final version

Title:	Checklist for Cloud Service Contracts
Status:	**FINAL**
Version:	2.0
Date submitted:	October 2015
Last reviewed:	February 26, 2016
Author:	InterPARES Trust Project
Writer(s):	Jessica Bushey, Marie Demoulin, Elissa How and Robert McLelland
Research domain:	North American Team – Legal – NA14

The following Checklist for Cloud Service Contracts is the final product of research being conducted by the InterPARES Trust Project on current cloud service contracts from a records management, archival, and legal perspective. InterPARES Trust (2013-2018) is a multi-national, interdisciplinary research project exploring issues concerning trust in digital records and data in the online environment. For more information see: https://interpares.org.

The target audience for this document is records managers, archivists, chief information officers, and others who are assessing cloud services for their organization. The aim of this document is to provide a tool to:

- gain an understanding of boilerplate cloud service contracts;
- verify if potential cloud service contracts meet their needs;
- clarify recordkeeping and archival needs to legal and IT departments;
- communicate recordkeeping and archival needs to cloud service providers.

This checklist is a tool for consideration only and does not constitute legal advice. We do not recommend for or against any particular cloud service provider (or the use of cloud services in general). Individuals and organizations should consult legal counsel if they want legal advice on a particular contract.

Checklist for Cloud Service Contracts Intended Audience: Records Managers and Archivists[1]				
Question	**Y**	**N**	**?[2]**	**Notes**
1. Agreement				
▪ Is the effective start date of the agreement clearly stated?				
▪ Is there an explanation of circumstances in which the services could be suspended?				
▪ Is there an explanation of circumstances in which the services could be terminated? (See also Section 8)				
▪ Is there an explanation of notification, or an option to subscribe to a notification service, in the event of changes made to the terms governing the service?[3]				
2. Data Ownership and Use				
▪ Do you retain ownership of the data that you store, transmit, and/or create with the cloud service?				
▪ Does the Provider reserve the right to use your data for the purposes of operating and improving the services?				
▪ Does the Provider reserve the right to use your data for the purposes of advertising?				
▪ Does the Provider reserve the right to use, or make your data available as anonymized open data (through standard APIs)?				

[1] The Checklist is primarily a tool for assisting organizations in assessing typical issues in boilerplate cloud computing legal agreements, in which the organization has to deal with legal agreements proposed by the Provider. The secondary application of the Checklist is to provide an overview of recordkeeping issues that are relevant to cloud computing services and should be addressed in the terms of the agreement. It is strongly recommended that any organization proceeding with the procurement of cloud computing services, in which a custom contract is being drafted, should carefully review and obtain all necessary legal advice on the specific terms of use.

[2] The "?" column indicates a situation in which the contract is unclear, or the question is not applicable to your situation.

[3] Some cloud service agreements, especially services in the public cloud, include clauses allowing the provider to change the terms of the agreement at any time at their sole discretion. Therefore, if possible, organizations should consider deleting this right, or making this right subject to the organization's agreement to any change, or ensuring the Provider is obligated to notify the organization well in advance of any changes.

▪ Does the Provider's compliance with copyright laws and other applicable intellectual property rights restrict the type of content you can store with the cloud service?				
▪ Do the Provider's terms apply to metadata?[4]				
▪ Do you gain ownership of metadata generated by the cloud service system during procedures of upload, management, download, and migration?				
▪ Do you have the right to access these metadata during the contractual relationship? (See also Section 8)				
3. Availability, Retrieval, and Use				
▪ Are precise indicators provided regarding the availability of the service?				
▪ Does the degree of availability of the data meet your business needs?				
▪ Does the degree of availability of the data allow you to comply with freedom of information (FOI) laws?[5]				
▪ Does the degree of availability of the data allow you to comply with the right of persons to access their own personal data?[6]				
▪ Does the degree of availability of the data allow you to comply with the right of authorities to legally access your data for investigation, control, or judicial purposes?				
▪ Are the procedures, time, and cost for restoring your data following a service outage clearly stated?				
4. Data Storage and Preservation				
4.1. Data Storage				
▪ Does the Provider create backups of your organization's data?				
▪ If your organization manages external records (e.g., customer data), does the Provider create				

[4] Metadata ensure that records can be discovered, retrieved and used. They are critical for ensuring the authenticity of the record over time. They can be generated by your organization or by the Provider. It is therefore important to specifically address metadata in the contract in order to clarify issues such as ownership, access, retention and disposition during the service and after its termination.

[5] In general, freedom of information laws allow access by the general public to information held by national governments.

[6] In some countries there is a Privacy Act to protect the privacy of individuals with respect to personal information about themselves held by public *and/or* private bodies, and provide individuals with a right of access to that information.

backups of your customer's data?				
▪ Do the Provider's terms apply to any backup created?[7]				
▪ In the event of accidental data deletion, does the Provider bear responsibility for data recovery?				
4.2. Data Preservation				
▪ Are there procedures outlined to indicate that your data will be managed over time in a manner that preserves their usability, reliability, authenticity, and integrity?[8]				
▪ Are there procedures to ensure file integrity during transfer of your data into and out of the system (e.g., checksums)?				
▪ Is there an explanation provided about how the service will evolve over time (i.e., migration and/or emulation activities)?				
▪ Does the system provide access to audit trails concerning activities related to evolution of the service?				
▪ Will you be notified by the Provider of changes made to your data due to evolution of the service?				
▪ Can you request notification of impending changes to the system related to evolution of the service that could impact your data?				
5. Data Retention and Disposition				
▪ Are you clearly informed about the procedure and conditions for the destruction of your data?[9]				
▪ Will your data (and all their copies, including backups) be destroyed in compliance with your data retention and disposition schedules?				
▪ If so, will they be immediately and permanently destroyed in a manner that prevents their reconstruction, according to a secure destruction policy ensuring confidentiality of the data until their complete deletion?				
▪ Is there information available about the nature				

[7] Notably in terms of ownership, access, security, retention and disposition during the service and after its termination.
[8] Usability, reliability, authenticity and integrity might be defined in the contract (e.g., in a Definition section or in a Glossary). It is recommended to verify if your organization and the Provider have a common understanding of these concepts.
[9] For example, is this operation automatic or does it require your authorization? Does the Provider offer a "freeze" function to temporarily suspend the disposition of a group of data and/or metadata against the instructions of the disposition schedule? Will you be made aware of, or are you able to specify, the method of disposition?

and content of the associated metadata generated by the cloud service system?				
▪ Will the Provider destroy associated metadata upon disposition of your data?				
▪ Will the Provider deliver and/or give access to audit trails of the destruction activity?				
▪ Will the Provider supply an attestation, report, or statement of deletion (if required by your internal or legal destruction policies)?				
6. Security, Confidentiality, and Privacy				
6.1. Security				
▪ Does the system prevent unauthorized access, use, alteration, or destruction of your data?				
▪ Is your data secure during procedures of transfer into and out of the system?				
▪ Does the system provide and give you access to audit trails, metadata, and/or access logs to demonstrate security measures?				
▪ Will you be notified in the case of a security breach or system malfunction?				
▪ Does the Provider use the services of a subcontractor?				
▪ Does the Provider offer information about the identity of the subcontractor and its tasks?				
▪ Are subcontractors held to the same level of legal obligations as the Provider of the cloud service?				
▪ Is a disaster recovery plan available or does the contract consider what happens in the event of a disaster?				
▪ Does the Provider offer any information regarding past performance with disaster recovery procedures?				
6.2. Confidentiality				
▪ Does the Provider have a confidentiality policy in regards to its employees, partners, and subcontractors?				
6.3. Privacy				
▪ Does the Provider's terms include privacy, confidentiality, or security policies for sensitive, confidential, personal or other special kinds of data?				

▪ Is it clearly stated what information (including personal information[10]) is collected about your organization, why it is collected and how it will be used by the Provider?				
▪ Does the Provider share this information with other companies, organizations, or individuals without your consent?				
▪ Does the Provider state the legal reasons for which they would share this information with other companies, organizations, or individuals?[11]				
▪ If the Provider shares this information with their affiliates for processing reasons, is this done in compliance with an existing privacy, confidentiality, or security policy?				
6.4. Accreditation and Auditing				
▪ Is the Provider accredited with a third party certification program?				
▪ Is the Provider audited on a systematic, regular, and independent basis by a third-party in order to demonstrate compliance with security, confidentiality, and privacy policies?				
▪ Is such a certification or audit process documented?				
▪ Do you have access to information such as the certifying or audit body and the expiration date of the certification?				
7. Data Location and Cross-border Data Flows				
7.1. Data Location				
▪ Do you know where your data and their copies are located while stored in the cloud service?				
▪ Does it comply with the location requirements that might be imposed on your organization's data by law, especially by applicable privacy law?				
▪ Do you have the option to specify the location, in which your data and their copies will be stored?				
▪ Do you know where metadata are stored and whether they are stored in the same location as your data?				

[10] Including personal information about your employees, customers, partners, providers, collaborators, etc.
[11] For example, do you know that your information may be accessible to law enforcement and national security authorities of different jurisdictions?

7.2. Cross-border Data Flows				
▪ Will you be notified if the data location is moved outside your jurisdiction?				
▪ Is the issue of your stored data being subject to disclosure orders by national or foreign security authorities addressed?				
▪ Does the Provider clearly state the legal jurisdiction in which the agreement will be enforced and potential disputes will be resolved?				
8. End of Service – Contract Termination[12]				
▪ In the event that the Provider terminates the service, will you be notified?				
▪ Is there an established procedure for contacting the Provider if you wish to terminate the contract?				
▪ If the contract is terminated, will your data be transferred to you or to another Provider of your choice in a usable and interoperable format?				
▪ Is the procedure, cost, and time period for returning/transferring your data at the end of the contract clearly stated?				
▪ At the end of the contract, do you have the right to access the metadata generated by the cloud service system?				
▪ At the end of the contract and after complete acknowledgement of restitution of your data, will your data and associated metadata be immediately and permanently destroyed, in a manner that prevents their reconstruction?				
▪ Is there an option for confirmation of deletion of records and metadata by the organization prior to termination of services with the Provider?				
▪ Is there an option for the client to terminate the service agreement without penalty in the event that the Provider of the cloud service changes?				

[12] The end of the service is a key moment that needs to be addressed in the contract in order to specify the procedure to follow, the obligations and responsibilities of both parties and the destination of all data before the contractual relationship is terminated.