

Checklist:

Cloud Service Contracts

*For Review*

*Draft v.1.2*

This work is made available through a **Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License**

 <http://creativecommons.org/licenses/by-nc-sa/4.0/>

|  |  |
| --- | --- |
| Title: | Checklist for Cloud Service Contracts |
| Status: | **DRAFT**  |
| Version: | 1.2  |
| Date submitted: | May 2015 |
| Last reviewed: | May 2015 |
| Author: | InterPARES Trust Project |
| Writer(s): | Jessica Bushey, Marie Demoulin, Elissa How and Robert McLelland |
| Research domain: | North American Team – Legal – NA14 |

**Draft version – For feedback**

The following Checklist for Cloud Service Contracts Draft v.1.2 is the draft 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.

Records managers, archivists, chief information officers, and others are invited to provide feedback to the Project 14 Team for the purposes of revision of the final Checklist (examples of feedback: clarity of a question, question to be added…).

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.

**Feedback should be provided before December 7th, 2015 to Corinne Rogers, iTrust Project Coordinator, corinne.rogers@ubc.ca.**

|  |
| --- |
| **Draft Checklist for Cloud Contracts** **Intended Audience: Records Managers and Archivists** |
| **Question** | **Y** | **N** | **?[[1]](#footnote-1)** | **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 automatic notification, or an option to subscribe to a notification service, in the event of changes made to the terms governing the service?
 |  |  |  |  |
| **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’s compliance with copyright laws restrict the type of content you can store with the cloud service?[[2]](#footnote-2)
 |  |  |  |  |
| * Do you gain ownership of metadata generated by the 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?[[3]](#footnote-3)
 |  |  |  |  |
| * Does the degree of availability of the data allow you to comply with the right of persons to access their own personal data?[[4]](#footnote-4)
 |  |  |  |  |
| * 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 customer data?
 |  |  |  |  |
| * 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?
 |  |  |  |  |
| * 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** |
| * Will your data (and all their copies) 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?
 |  |  |  |  |
| * Are you aware of the nature and content of the associated metadata generated by the 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 through technical, physical, and organization measures?
 |  |  |  |  |
| * 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?
 |  |  |  |  |
| * Is there a disaster recovery plan available?
 |  |  |  |  |
| *6.2. Confidentiality* |
| * Does the Provider have a confidentiality policy in regards to its employees, partners, and subcontractors?
 |  |  |  |  |
| *6.3. Privacy* |
| * Are there privacy, confidentiality, or security policies for sensitive, confidential, personal or other special kinds of data you store with the Provider?
 |  |  |  |  |
| * Does the system prevent unauthorized access, use, alteration, or destruction of your personal information through technical, physical, and organizational measures?
 |  |  |  |  |
| * Is it clearly stated what personal information is collected and why it is collected?
 |  |  |  |  |
| * Is it clearly stated how the personal information collected will be used?
 |  |  |  |  |
| * Does the Provider share your personal information with other companies, organizations, or individuals without your consent?
 |  |  |  |  |
| * Does the Provider clearly state the legal reasons it which they would share your personal information with other companies, organizations, or individuals?
 |  |  |  |  |
| * If the Provider shares your personal information with their affiliates for processing reasons, is this done in compliance with a 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?
 |  |  |  |  |
| *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** |
| * 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 will be transferred to you in a usable and interoperable format?
 |  |  |  |  |
| * Is the procedure, cost, and time period for returning your data at the end of the contract clearly stated?
 |  |  |  |  |
| * At the end of the contract, do you have the right to access the associated metadata generated by the 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?
 |  |  |  |  |

1. The “?” column indicates a situation in which the contract is unclear, or the question is not applicable to your situation. [↑](#footnote-ref-1)
2. For example, the Digital Millennium Copyright Act (USA). [↑](#footnote-ref-2)
3. In general, freedom of information laws allow access by the general public to information held by national governments. [↑](#footnote-ref-3)
4. 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. [↑](#footnote-ref-4)