

InterPARES Trust Project Report



Title and code:	The impact of the Italian legal framework for cloud computing on electronic recordkeeping and digital preservation system - EU 35
Document type:	Final report
Status:	Final Version
Version:	1
Research domain:	Legal
Date submitted:	January 10, 2018
Last reviewed:	
Author:	InterPARES Trust Project
Writer(s):	Stefano Allegrezza, Gabriele Bezzi, Maria Mata Caravaca, Maria Guercio, Ilaria Pescini, Brizio Tommasi
Research team:	European Team

Document Control

Version history			
Version	Date	By	Version notes
1	2017/12/12	Maria Guercio	
2	2018/01/02		Revision by the other authors
3	2018/01/05	Maria Guercio	
4	2018/01/07		Revision by the other authors
5	2018/01/10	Maria Guercio	Final version

Table of Contents

Abstract or Executive Summary	4
Research team	4
Background.....	4
Research questions	4
Aims and Objectives/Goals	4
Methodology	5
Findings	5
Conclusions.....	10
References.....	11

Abstract or Executive Summary

The proposal analyses the recent Italian legislation and policies for a large use of cloud computing services in the public sector and intends to assess their peculiarities against the crucial requirements identified at national and international levels for qualified recordkeeping and digital preservation systems. To assess the Italian legal framework and the common practice (based on four case studies) the team adopted the checklist developed within iTrust for analyzing cloud services contracts (Study NA14) and tested it in 4 case studies. The whole study is related to the objective no. 3 of InterPARES Trust project.

The impact of the Italian legal framework for cloud computing on electronic recordkeeping and digital preservation system - Code 35

Research team

Lead Researcher: Maria Guercio

Project Researchers: Stefano Allegrezza, Gabriele Bezzi, Maria Mata Caravaca, Ilaria Pescini, Brizio Tommasi

Within InterPARES team the institutions involved are: Digilab, Regione Toscana and Regione Emilia Romagna, ICCROM, Consob and the University of Udine.

Background

The project analyses the recent Italian legislation and policies for the large use of cloud computing services in the public sector and takes into account the outputs achieved by other I-Trust studies and specifically Cloud Contracts Checklist (Code NA14).

Research questions

The research question at the basis of the study concerns the objective no. 3 of I-Trust project: "What significance do national/cultural context have on trust in digital records".

The questions involved in the study concern:

- the relation of the Italian recommendations for cloud computing with the relevant and consolidated principles recognized at international level and adopted by the Italian legislation in the field of recordkeeping system and digital preservation;

- the usefulness of the checklist developed by InterPARES –Trust project at national level.

Aims and Objectives/Goals

The proposal intends to verify – against a checklist already developed by InterPARES Trust researchers – the level of control already in place according to the Italian legislation and policies in adopting cloud services. A second goal concerns the analysis of the common practice in four different case studies related to the application of cloud services. Three of them concern Italian public sector, while a third one is related to ICCROM, an international body.

Methodology

The researchers adopted two types of actions: a survey of the Italian legislation and policies conducted on the basis of the Cloud Contracts Checklist (Code NA14) and the assessment (against the checklist) of three case studies of institutions where cloud services have been already implemented for some specific areas.

The survey uses the analysis already developed in the previous project EU4 (*Policies for recordkeeping and digital preservation. Recommendations for analysis and assessment services*)

Findings

1. State of art and legal frameworks in Italy on recordkeeping and preservation systems played with cloud services

As already mentioned in the description of the methodology, the survey started with the conclusion of the previous study dedicated to the analysis of the legal framework for recordkeeping and digital preservation in Italy where a specific legislation “able to provide rules for governing cloud systems (at least for the public administration) is not yet in place, but the general framework for electronic records keeping systems and digital preservation systems (and also for the public contracts) is consistent enough to support future risks in cloud environment”.

Because of the lack of a dedicated legislation on cloud services for public administrations, the researchers have identified a list of rules and policies useful at different levels for describing the framework to consider when recordkeeping and preservation functions are implemented as cloud services. For this purpose, various categories of rules are relevant, all of them consistent with the guidelines approved in

Europe within the project Cloud for Europe (www.agid.gov.it/cloudforeurope) which uses pre-commercial procurement as an instrument for public sector innovation¹:

- a. specific policies, recommendations and guidelines focused on the use of cloud computing in the public sector (without reference to the recordkeeping and preservation systems): *Raccomandazione e proposte sull'utilizzo del cloud computing nella pubblica amministrazione*, DigitPA, 2012, www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cloud-computing; *Caratterizzazione dei sistemi cloud per la pubblica amministrazione*, Agid, 2013, www.agid.gov.it/notizie/2013/10/16/linee-guida-le-soluzioni-cloud-spc. Many obligations are part of the general legislation on public procurement (decree of the President of Republic 207/2010).

At the moment these rules imply that the storage for digital preservation must be located in Italy to allow audit by national authorities (Agid). New regulations are under development and seem to consider the possibility of locating the main system outside the national territory if at least 'a copy' of the records/information is kept in Italy (draft of the Code for Digital Administration, 2017).

National plans (such as the digital Agenda plan 2017-2020: *Three-Year Plan For Ict In Public Administration 2017 - 2019* <https://pianotriennale-ict.readthedocs.io/en/latest/>) define policy and strategic programs which could be relevant for defining frameworks and requirements for cloud computing. More specifically the digital Agenda approved in 2017 defines a policy for regionalization of data centers in the public sector: a small number of national data centers and preservation centers will be identified at the end of the project (December 2018) and will be able to support the public services delivered in cloud systems. The Central Archives of the State and public preservation centers such as those developed by some Regions will be also included in this list. The Agenda and specific project include also the realization of a private cloud for public administrations data and records. From a general point of view the Agenda includes also a new perspective for the use of cloud computing in Italy and a model in the public sector (SPC Cloud Tender) whose characteristics will be considered in detailing the compliance of the national system with the iTrust checklist. The Plan will develop along three main directions:

- the reorganisation of the public administration data centres through rationalisation work, both to reduce management costs and adapt and increase the quality of services offered to public administrations, including in terms of business continuity, disaster recovery and energy efficiency;

¹ The problems related to the procurement are very complex in Europe and even more in Italy. It will not be analyzed in details in this report, but only with reference to the checklist specific requirements.

- the implementation of the PA cloud, enabling virtualisation of the machinery of all public administrations, with significant maintenance and cost management benefits. Cloud services will be offered in IaaS (Infrastructure as a Service) PaaS (Platform as a Service) and SaaS (Software as a Service) modes;
- the rationalisation of public administration connectivity costs and the increase in the spread of connectivity in public places for the benefit of citizens.

The Plan has the aim to Create a PA cloud environment, homogeneous from the contractual and technological point of view, by retraining internal resources existing in PAs or by resorting to resources of qualified external parties, with the use of public and private *cloud* for *storage* and computing and the systematic adoption of the cloud paradigm.

- b. The main part of the legislation (in the form of acts, regulations and guidelines) concerning cloud services for RKS and digital preservation exists in areas not directly related to cloud computing. More specifically, the rules are present in the general legislation related on procurement and tenders for the public sector, while a new area for audit and control is under development thanks to the initiative of ANAC – National Authority for Transparency and Accountability. The rules in questions include: the legislation on recordkeeping systems (decree of President of Republic 445/2000 and related regulations approved with a decree of Prime Minister 3 December 2013); the legislation on digital preservation (Code of Digital Administration approved with a legislative decree 82/2005 and continuously updated) and its regulation approved with another decree of Prime Minister 3 December 2013); guidelines adopted by Agid with specific reference to audit and certification of digital repositories (circolare 65/2014, *Accreditamento dei soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici per conto terzi, Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza*, www.agid.gov.it/sites/default/files/documentazione/requisiti_di_qualita_e_sicurezza_v.1.1.pdf and *Linee guida per la conservazione dei documenti informatici*, www.agid.gov.it/sites/default/files/linee_guida/la_conservazione_dei_documenti_informatici_rev_def.pdf).

2. The comparison with iTrust checklist

On the basis of the previous analysis of the Italian legislation, the checklist adopted by iTrust was the framework for assessing the fragmented and complex Italian legislation on current cloud service contracts from a records management, archival, and legal perspective. Because of the comprehensive nature of the checklist, not all the questions there included are relevant per se or could play a meaningful role for the specific case studies chosen in the part of the report (such as those focused on the definition of

individual agreements), but the team has considered the usefulness of the checklist by taking into account the Italian general.

For this reason, the checklist was here used as a list of crucial questions to be considered and answered first of all by analyzing the national framework and secondly in each checklist area (1. Agreement, 2. Data ownership and use, 3. Availability, retrieval and use, 4. Data storage and preservation, 5. Data retention and disposition, 6. Security, confidentiality and privacy, 7. Data location and cross-border data flows and 8. End of service – contract termination). The Italian legislation does not consider all these questions and for this reason the team had to adapt the checklist or, better, to limit the elements of the checklist to compare with the present national framework. The report includes the main finding from this comparison:

1. Agreement
2. Data ownership and use
3. Availability, retrieval and use
4. Data storage and preservation
5. Data retention and disposition
6. Security, confidentiality and privacy
7. Data location and cross-border data flows
8. End of service – contract termination

<p>1. Agreement</p>	<p>All the questions involved are ruled in the Italian legislation by the regulation on digital preservation (decree 3.12.2013 which states the obligation of specific agreement for any services related to the digital archiving in the public sector, but also in case of private records; the decree in question implies the definition of a very specific and detailed manual which includes responsibilities, terms of services, level of interoperability, etc. The Agency in charge with the control, Agid, has defined a prototype (see the index in appendix) for all the repositories which require certification and intend to preserve public records</p>
<p>2. Data ownership and use</p>	<p>Also in this case the regulation mentioned at point 1 is quite inclusive and precise: agreements must be in place; the ownership is well defined by the general Italian legislation; the technical issues are regulated in details only when public data and records are preserved by third parties. In this case Agid policies and guidelines are very strict and all the crucial aspects are considered in compliance with standards OAIS and ISO 16363. With reference to the metadata issues (for interoperability, but also for access and for privacy) have been identified in the rules for recordkeeping (decree 445/2000; decree 3.12.2013) and in the legislation dedicated to the creation of electronic records (Code of Digital Administration</p>

	and regulation 13.11.2014). A national standard is also in place for ensuring interoperability, even if this standard (UniSincro) has too many areas not well detailed.
3. Availability, retrieval and use	This area is generally present in the manuals and there is specific obligation for all the repositories asking for accreditation, but there is no evidence, at the moment, of their compliance with the requirements included in the checklist. The legal term in the national legislation “esibizione” is clearly defined in the regulations and is always handled by the formal manuals
4. Data storage and preservation	All the repositories certified as trusted repositories against the specific legislation must be compliant with all the relevant standards for security and preservation; because of the obligatory compliance with OAIS and ISO 16363 all the relevant questions related to the authenticity and integrity and their documentation and evidence are included in the fundamental requirements the repositories have to meet
5. Data retention and disposition	This sector has been regulated by the National Archives (circulars 40 and 41/2015 but also decree 445/2000) in compliance with the general archival legislation (Codice dei beni culturali). The controls are very strict for the public sector.
6. Security, confidentiality and privacy	<p>All the requirements are part of the general obligations of the repositories in charge of keeping public records. However, some specific rules imply the capacity of the records creators to be active in controlling and assessing the quality of the service. Many creators (such as the municipalities and local authorities) have no technical capacity for a proactive control of these requirements.</p> <p>The privacy sector (6.3) is strictly ruled according to the Italian and European legislation. A special agency has a powerful capacity of controlling the respect of the rules in place. Accreditation and auditing (6.4) are very well defined with reference to the digital records created by the public administration. See the circulars and the guidelines adopted by Agid and mentioned in the previous part of this report: circolare 65/2014, <i>Accreditamento dei soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici per conto terzi, Requisiti di qualità e sicurezza per l'accREDITamento e la vigilanza</i>, www.agid.gov.it/sites/default/files/documentazione/requisiti_di_qualita_e_sicurezza_v.1.1.pdf and <i>Linee guida per la conservazione dei documenti informatici</i>, www.agid.gov.it/sites/default/files/linee_guida/la_conservazi</p>

	<i>one dei documenti informatici rev def.pdf</i>
7. Data location and cross-border data flows	At the moment, as already mentioned in the report, the location of data must include only the national boundaries. In the new strategic plan under development a new rule (not yet clarified) seems to allow for an international data location with the condition that at least one copy must be retained in Italy
8. End of service – contract termination	This issue is explicitly ruled In the legislation and on this basis must be defined in each specific agreement. It is not clear if the rules are sufficiently convincing.

3. The case studies

As mentioned earlier, the framework has been considered useful for assessing some specific cases and agreements. Of course, when the framework is adopted to analyze single and very specific situations and contracts many issues are not relevant or applicable.

The case studies here presented concern:

- Regione Emilia Romagna (annex 1): the contract for the use in cloud of Office 365 and the agreement for long-term digital preservation services;
- Regione Toscana (annex 2): the contracts implemented for the Toscana community in relation to the use of the private cloud computing system TIX and its related ICT services;
- University of Udine (annex 3): the contract to use Microsoft Azure Virtual Machine services to execute machine learning solutions;
- ICCROM (annex 4): the contract signed to use Azure, the Microsoft cloud service, required for supporting the proprietary financial accounting system SAP.

All the case studies, even if related to different areas and types of services, testify the same kind of criticalities: a very limited attention for the risks of records, of authenticity and integrity of the information involved in the services. When standard contracts are in place the main issues are related to the contractual/commercial aspects and legal restriction (such as pricing, and payment, renewal, agreement term, termination and suspension, warranties, claims, limitations of liability, obligations). The technical storage is also considered from a very limited point of view: data location, security, confidentiality and privacy are the basic aspects under control. The only exception has been the agreement approved by Regione Emilia Romagna for its digital preservation service, where the nature of the function has implied a serious attention for the archival aspects and has proved the usefulness of the iTrust checklist.

Conclusions

The project work and its findings testify (from many points of view) the need for a more precise and detailed effort when cloud services are in place. It also confirms the relevance of a common checklist to analyze complex functions. The international nature of the checklist was not a negative aspect and could be easily applied to the national environment. The comparison was very fruitful when specifically referred to the recordkeeping and digital preservation dimension. On the opposite, when used for the exam of contracts not specifically related to the recordkeeping or when the officers in place did not pay attention to these aspects in developing cloud systems and accept standard no-negotiated contracts, the checklist seems *mute*: the researchers had difficulties in describing the lack of attention. Nevertheless, also in this case the exercise was useful because it makes explicit the relevant risks in place when record managers or archivists are not consulted and the lack of awareness of the other sectors in the organizations, even when they are used to be compliant with archival standards.

References

M. Guercio, *The Italian case: legal framework and good practices for digital preservation*, in *CULTURAL HERITAGE on line – “Trusted digital repositories & trusted professionals. Firenze 11-12 December 2013*, Firenze, 2013,

EU4 (*Policies for recordkeeping and digital preservation. Recommendations for analysis and assessment services*)

Forum PA, Cloud Computing, quali scenari per la Pubblica Amministrazione, 28 aprile 2011 <http://www.forumpa.it/cloud-computing-quali-scenari-per-la-pubblica-amministrazione-on-line-gli-atti>

I-Trust Checklist for Cloud Service Contracts, final version, 2016

ISO/TC46/SC!! Call for expert(s) -WG17 Cloud in Records – Preliminary work item (TR) – ISO/WI/DTR – Information and documentation – Records management in cloud: issues and concerns, 2016

NIST Cloud Computing Program, Cloud computing and accessibility considerations R.B. Bhon, J Tobias eds), 2016, <https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp>