

# MANUALE DI CONSERVAZIONE

*(DPCM 3 dicembre 2013, art. 8)*

Questo manuale è stato redatto, sulla base del modello del progetto del Gruppo di lavoro *Procedamus*, da Giorgio Piermarini, Responsabile della Conservazione dell'Università per Stranieri di Perugia.

*Edizione - maggio 2019*  
*Emanato con Decreto D.G. 30 maggio 2019, n. 199*  
*Aggiornato in data 23 giugno 2025*

# INDICE

## Premessa

### Scopo e ambito del documento

1. Il processo di Conservazione Sostitutiva di Cineca
  - 1.1. Modello organizzativo della Conservazione: Ruoli e Responsabilità
    - 1.1.1. Il modello organizzativo adottato
    - 1.1.2. Soggetto Produttore
    - 1.1.3. Organigramma
    - 1.1.4. Struttura organizzativa
    - 1.1.5. Utente
    - 1.1.6. Responsabile della conservazione
    - 1.1.7. Organismi di tutela e vigilanza
  - 1.2. Organizzazione del Servizio di conservazione
    - 1.2.1. Responsabilità del sistema di conservazione
    - 1.2.2. Gestione del sistema di conservazione: Organigramma, Struttura organizzativa, Pubblico ufficiale
  - 1.3. Oggetti sottoposti a conservazione
    - 1.3.1. Documenti informatici e loro aggregazione: Serie e relativi Repertori
    - 1.3.2. Unità archivistiche e unità documentarie
    - 1.3.3. Formati
    - 1.3.4. Metadati
    - 1.3.5. Pacchetto informativo: Pacchetto di versamento, di archiviazione, di distribuzione
  - 1.4. Processo di conservazione
    - 1.4.1. Fasi del versamento e logiche di conservazione
    - 1.4.2. Acquisizione e presa in carico dei pacchetti di versamento (SIP)
    - 1.4.3. Gestione del pacchetto di archiviazione (AIP)
    - 1.4.4. Gestione del pacchetto di distribuzione (DIP)
    - 1.4.5. Monitoraggio e risoluzione delle anomalie
  - 1.5. Descrizione del sistema di conservazione
    - 1.5.1. Componenti Logiche
    - 1.5.2. Componenti Fisiche
    - 1.5.3. Componenti Tecnologiche
    - 1.5.4. Procedure di gestione del sistema
    - 1.5.5. Evoluzione del sistema
    - 1.5.6. Monitoraggio e controlli
  - 1.6. Strategie adottate a garanzia della conservazione
    - 1.6.1. Misure a garanzia della intellegibilità, della leggibilità e della reperibilità nel tempo
    - 1.6.2. Misure a garanzia dell'interoperabilità e della trasferibilità ad altri conservatori
  - 1.7. Trattamento dei dati personali
2. Il processo di Conservazione Sostitutiva di UniIT
  - 2.1. Descrizione del servizio
    - 2.1.1. Acquisizione dei pacchetti di versamento e presa in carico
    - 2.1.2. Ricezione dell'indice del pacchetto di versamento

- 2.1.3. Ricezione documenti associati ad un pacchetto di versamento
- 2.1.4. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico
- 2.1.5. Preparazione e gestione del pacchetto di archiviazione
- 2.1.6. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione
- 2.2. L'Architettura e l'infrastruttura
  - 2.2.1. Infrastruttura Informatica
  - 2.2.2. Caratteristiche generali della soluzione di conservazione
  - 2.2.3. Affidabilità - Totale ridondanza ai guasti HW
  - 2.2.4. Architettura fisica
- 2.3. Certificazioni UniIT
  - 2.3.1. ISO IEC 20000-1:2011
  - 2.3.2. UNI CEI ISO/IEC 27001:2014
  - 2.3.3. UNI EN ISO 9001:2015

## ALLEGATI

Allegato 1: Normativa di riferimento

Allegato 2: Denominazione UOR afferenti alla AOO "Amministrazione centrale"

Allegato 3: Nomina del Responsabile della Conservazione per l'Università per Stranieri di Perugia

Allegato 4: Nomina e Compiti ai quali deve attenersi il Responsabile esterno al trattamento dei dati personali, ed Elenco delle tipologie documentarie soggette a conservazione, per quanto concerne CINECA

Allegato 5: Convenzione di Affidamento del Servizio di Conservazione, Nomina e Adempimenti del Responsabile esterno del Trattamento dei dati personali, e Affidamento all'esterno delle attività del Responsabile della conservazione, per quanto concerne UniIT

Allegato 6: Accordi di versamento e Manuale del Conservatore, per quanto concerne CINECA, e Manuale del Conservatore per quanto concerne UniIT

## **Premessa**

La Conservazione è una procedura informatica regolamentata dalla legge italiana che, attraverso l'adozione di regole, procedure e tecnologie, consente di garantire nel tempo le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti (art. 44 del CAD).

Il DPCM del 3 dicembre 2013 contiene le Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al D.lgs. n. 82 del 2005.

Pubblicato in Gazzetta Ufficiale il 13 marzo 2014 e divenuto esecutivo un mese dopo, il suddetto decreto va ad aggiornare quanto precedentemente indicato dalla delibera CNIPA n. 11/2004 e introduce il concetto di "sistema di conservazione", che assicura la conservazione a norma dei documenti elettronici e la disponibilità dei fascicoli informatici, stabilendo le regole, le procedure, le tecnologie e i modelli organizzativi da adottare per la gestione di tali processi.

Il DPCM, inoltre, disciplina in modo più accurato la figura del Responsabile della Conservazione, del Produttore e degli Utenti.

La Circolare n°65 /2014 AgID stabilisce infine le modalità per l'accreditamento e per la vigilanza dei soggetti che intendono conseguire i riconoscimenti più elevati in termini di qualità e sicurezza prevedendone l'iscrizione in un apposito elenco pubblico.

## **Scopo e ambito del documento**

Il manuale di conservazione (d'ora in poi "manuale") dei documenti digitali, come previsto dall'art. 7, comma 1, lettera m e dall'art. 8 del DPCM 3 dicembre 2013, è uno strumento operativo che descrive e disciplina il modello organizzativo adottato per la conservazione.

Esso illustra nel dettaglio l'organizzazione del processo di conservazione, definendo i soggetti coinvolti e i ruoli svolti dagli stessi nel modello organizzativo di funzionamento dell'attività di conservazione dall'Università per Stranieri di Perugia come soggetto produttore (d'ora in poi "Produttore") che intende sottoporre a conservazione digitale fascicoli, serie e aggregazioni documentali, affidando il processo di conservazione al Consorzio interuniversitario – CINECA, nonché sottoporre a conservazione digitale i documenti contabili, affidando il processo di conservazione alla UniIT S.r.l. – Gruppo Bancario UniCredit S.p.A. (d'ora in poi "Conservatori").

La redazione del manuale di conservazione contempera l'assolvimento dell'obbligo normativo con le esigenze concrete del Produttore.

Il manuale costituisce una guida per gli attori coinvolti nel processo di gestione e di conservazione, per il cittadino e per le imprese. Ai primi, per porre in essere le corrette operazioni di gestione e conservazione documentale, agli ultimi due per comprendere le caratteristiche del Sistema di conservazione documentale e dei processi erogati.

Il manuale descrive inoltre il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento del Sistema di conservazione.

Per le tipologie degli oggetti sottoposti a conservazione e i rapporti con il Conservatore, il presente manuale è integrato con gli Accordi di versamento, che definiscono le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei documenti informatici e delle aggregazioni documentali informatiche oggetto di conservazione.

L'Accordo di versamento è formato da specifiche parti relative alle diverse tipologie documentarie oggetto di conservazione ed è compilato tenendo conto delle indicazioni contenute nella documentazione redatta rispettivamente da Cineca e da UniIT.

## **1. Il processo di Conservazione Sostitutiva di Cineca**

### **1.1. Modello organizzativo della Conservazione: Ruoli e Responsabilità**

#### **1.1.1. Il modello organizzativo adottato**

La scelta adottata dal Produttore è quella del modello in outsourcing (cioè affidare parzialmente o totalmente il servizio di conservazione a soggetti pubblici o privati accreditati ai sensi dell'art. 44-bis, comma 1 del CAD), per la fornitura del servizio di conservazione.

Il Produttore è il titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della conservazione, definisce e attua le politiche complessive del Sistema di conservazione governandone la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato affida al Conservatore la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia.

Il sistema di conservazione, denominato Conserva, agisce in piena ottemperanza alle direttive descritte nelle regole tecniche in materia di sistema di conservazione dei documenti informatici; segue, inoltre, lo standard di riferimento per la certificazione dei depositi digitali ISO 14721:2012 OAIS (Open Archival Information System).

#### **1.1.2. Soggetto Produttore**

L'Università per Stranieri di Perugia è il soggetto produttore che versa le unità documentarie informatiche da conservare con gli opportuni metadati, in continuità con il processo di gestione documentale, iniziato nella fase corrente all'interno dell'Ateneo.

I rapporti tra Produttore e Conservatore, cui è stata assegnata con atto di affidamento la gestione del servizio di conservazione, sono formalizzati e regolati per mezzo di alcuni documenti fondamentali:

- Accordo quadro tra Università e CINECA concluso in data 17/09/2012 di cui l'Ateneo è membro effettivo del Consorzio CINECA,
- Atto di affidamento dei servizi per l'utilizzo delle soluzioni Cineca (Confirma - Conserva - Integrazione con Procedamus) e dei servizi di assistenza connessi, Prot. n. 10106 e 10107 del 23/12/2015 (con estensione temporale dei servizi dal 01/04/2015).

Alla data di adozione del presente manuale sono stati stipulati gli accordi di versamento per le seguenti tipologie documentali:

- Registro giornaliero di protocollo,
- Fatture elettroniche attive,
- Fatture elettroniche passive,
- Registri IVA.

Il testo completo degli accordi è inserito nell'allegato n.5, contenenti i nominativi delle figure coinvolte e la descrizione delle principali attività svolte da coloro che hanno ruoli organizzativi all'interno del soggetto produttore e all'esterno.

#### **1.1.3. Organigramma**

L'Università è organizzata nelle AOO e UOR descritte nell'allegato n.2, come previsto dalla legge 7 agosto 1990, n. 241 (artt. 4 e 6), dal DPR 28 dicembre 2000, n. 445 e dal DPCM 3 dicembre 2013, art. 3, comma 1, lettera a).

L'area organizzativa omogenea (AOO) è l'insieme di funzioni e di strutture individuate dall'amministrazione cui sono assegnate funzioni omogenee. Essa, pertanto, presenta esigenze di gestione documentale in modo unitario e coordinato, ai sensi della normativa vigente.

L'unità organizzativa responsabile (UOR) è, all'interno della AOO, un complesso organizzato di risorse umane e strumentali cui è stata affidata una competenza omogenea nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari, attività e procedimenti amministrativi.

Per maggiori dettagli inerenti all'organigramma si rimanda all'allegato n.2 del presente manuale, e/o all'informativa reperibile nel sito d'Ateneo al link: [www.unistrapg.it](http://www.unistrapg.it).

Il versamento in conservazione dei documenti informatici gestiti nella fase corrente dalle articolazioni amministrative (AOO e UOR) del Produttore è effettuato unicamente dal Responsabile della conservazione, o dal suo delegato.

#### **1.1.4. Struttura organizzativa**

Il Sistema di conservazione delle unità documentarie informatiche e delle unità archivistiche informatiche di Ateneo, prevede la collaborazione tra unità organizzative e soggetti cui il Produttore ha affidato il coordinamento del processo di conservazione, in base all'atto di affidamento e relativi accordi di versamento nel quale sono inoltre definite le tipologie documentali, i tempi di versamento e conservazione, i formati e i metadati descrittivi utili a garantire una corretta interazione tra Produttore e Conservatore.

In virtù di tale affidamento del servizio di conservazione il Conservatore si impegna alla conservazione dei documenti trasferiti e ne assume la funzione di Responsabile del servizio di conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i Sistemi di conservazione, e svolge l'insieme delle attività elencate nell'art. 7 comma 1 delle Regole tecniche citate.

In particolare l'esecuzione del processo di conservazione avviene sotto la vigilanza del Responsabile della conservazione il quale interagisce con il Responsabile del servizio di conservazione del Conservatore.

#### **1.1.5. Utente**

Ai sensi dell'art. 6 del DPCM 3 dicembre 2013 *Regole tecniche in materia di Sistema di conservazione*, l'utente è la persona fisica o giuridica, interna o esterna al Sistema di conservazione, secondo il modello organizzativo adottato, che interagisce con i servizi di un Sistema di gestione informatica dei documenti e/o di un Sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse; in termini di sistema OAIS, la comunità degli utenti può essere definita come Comunità di riferimento.

L'utente finale del servizio di conservazione è lo stesso Ateneo che interagisce, tramite i propri funzionari autorizzati con il servizio di conservazione, per accedere ai documenti, per finalità gestionali, amministrative, storiche, scientifiche o per soddisfare le richieste di eventuali soggetti esterni legittimati all'esibizione/accesso alla documentazione (es: amministrazioni/enti pubblici, soggetti privati, aziende, professionisti, cittadini, stakeholder interni).

Il Sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un Pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.

Nel ruolo dell'utente, sono definiti gli specifici soggetti abilitati dell'Ateneo, in particolare gli operatori indicati dal Produttore e riportati negli accordi di versamento, che possono accedere esclusivamente ai documenti versati dal Produttore stesso o solo ad alcuni di essi secondo le regole di visibilità e di accesso concordate tra Produttore e Conservatore.

Si identificano gli utenti del Sistema di conservazione nelle seguenti persone:

- Responsabile della conservazione,
- Delegati del responsabile della conservazione.

L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione, e nel rispetto delle misure di sicurezza previste negli artt. da 31 a 36 del D.lgs. 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del medesimo Decreto.

Nell'ambito dell'Università per Stranieri di Perugia, sono stati nominati il dott. Giorgio Piermarini quale Responsabile della conservazione (D.D.G. n.66 del 14.3.2016) e il dott. Francesco Scolastra quale Delegato del responsabile della conservazione (comunicazione del 29.3.2016).

### **1.1.6. Responsabile della conservazione**

Il Responsabile della conservazione è la figura cardine che governa il processo della conservazione digitale: è la persona fisica inserita stabilmente nell'organico del soggetto produttore dei documenti, che definisce e attua le politiche complessive del Sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato; il Responsabile della conservazione può nominare i propri delegati. Nelle pubbliche amministrazioni il ruolo di Responsabile della conservazione può essere svolto dal Responsabile della gestione documentale, ovvero dal Coordinatore della gestione documentale, ove nominato.

Il Responsabile della conservazione, coadiuvato dal Responsabile del sistema di conservazione Conserva di Cineca, ha i seguenti compiti:

- accertare, con periodicità almeno annuale, la conformità del processo di conservazione alla normativa vigente;
- archiviare e gestire i rapporti di versamento prodotti da Conserva secondo le modalità descritte nel manuale di gestione;
- effettuare il monitoraggio del corretto funzionamento del Sistema di conservazione;
- assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- predisporre il manuale di conservazione e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Al Responsabile del sistema di conservazione Conserva sono affidate le specifiche funzioni e competenze di:

- definire le caratteristiche e i requisiti del Sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestire il processo di conservazione e garantire nel tempo la conformità alla normativa vigente;
- generare il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure con riguardo all'obsolescenza dei formati;
- adottare le misure necessarie per la sicurezza fisica e logica del Sistema di conservazione ai

sensi dell'art. 12 del DPCM 3 dicembre 2013;

- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione o in specifici accordi di versamento;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione.

Il Responsabile del servizio di conservazione si occupa delle politiche complessive del Sistema di conservazione e ne determina l'ambito di sviluppo e le competenze; a tal fine, anche in coerenza con OAIS, provvede alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e a ogni altra attività gestionale mirata a coordinare lo sviluppo del Sistema.

Il Responsabile della conservazione opera d'intesa con il Responsabile del servizio di conservazione, con il Responsabile del trattamento dei dati personali, con il Responsabile della sicurezza del sistema, con il Responsabile dei sistemi informativi e con il Responsabile della gestione documentale; in particolare ha il compito di:

- produrre il pacchetto di versamento secondo le regole pattuite tra Responsabile della conservazione e Conservatore;
- assicurare la trasmissione del contenuto del pacchetto di versamento nel rispetto di quanto definito, tra Responsabile della conservazione e Responsabile del servizio di conservazione, nel manuale di conservazione;
- effettuare l'analisi dei procedimenti amministrativi e una ricognizione delle tipologie documentali.

#### **1.1.7. Organismi di tutela e vigilanza**

Gli archivi e i singoli documenti prodotti dagli enti universitari sono beni culturali e sono sottoposti, pertanto, alle disposizioni di tutela previste dal Codice dei beni culturali; garantire la tutela di archivi e singoli documenti si concreta negli obblighi conservativi previsti nell'art. 30 del predetto Decreto Legislativo che comporta, infatti, "l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli ... I soggetti medesimi hanno altresì l'obbligo di inventariare i propri archivi storici". Il rispetto delle disposizioni in ordine alla corretta conservazione è in capo al Ministero dei beni e delle attività culturali e del turismo, attraverso la Direzione generale archivi e, in particolare, alla Soprintendenza archivistica e bibliografica dell'Umbria; tale ente, infatti, è investito del potere di vigilanza e ispezione.

Il legislatore ha previsto un secondo ente che, in materia di conservazione digitale, lavora a fianco delle Soprintendenze, avendo però un ruolo diverso. L'Agenzia per l'Italia digitale - AgID, infatti, per quanto concerne i sistemi di conservazione di archivi e documenti digitali, ha il compito di gestire il processo di accreditamento dei soggetti che richiedono di essere individuati come Conservatori, ai sensi dell'art. 29 – Qualificazione e accreditamento, del Codice dell'amministrazione digitale, e ai sensi dell'art. 13 – Accreditamento, delle Regole tecniche sul sistema di conservazione. AgID, quindi, definisce, con propri provvedimenti, le modalità per l'accREDITamento e vigila sui soggetti diventati Conservatori accreditati.

Il Sistema di conservazione di Cineca è sottoposto quindi alla vigilanza di AgID che prevede la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e l'accesso ai dati presso la sede del Produttore.

Per migliorare la qualità dell'intero processo di conservazione, il Produttore e il Conservatore possono avvalersi di specifici standard di valutazione, di autovalutazione e di auditing.

### **1.2. Organizzazione del Servizio di conservazione**

#### **1.2.1. Responsabilità del sistema di conservazione**

Il Sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Produttore, fino all'eventuale scarto, indipendentemente dall'evolversi del contesto tecnologico e organizzativo.

La responsabilità del Sistema di conservazione come soggetto che svolge attività di conservazione è in capo al Consorzio interuniversitario Cineca.

Cineca è un consorzio interuniversitario senza scopo di lucro, formato da 70 Università italiane, 6 enti di ricerca il Ministero dell'Istruzione, dell'Università e della Ricerca – MIUR; costituito nel 1969 come Consorzio Interuniversitario per il calcolo automatico dell'Italia Nord Orientale, oggi Cineca è il maggiore centro di calcolo in Italia.

La sua missione istituzionale comprende la realizzazione di sistemi gestionali e servizi a sostegno delle università e del Ministero dell'Istruzione, dell'Università e della Ricerca - MIUR. Per questo, il Consorzio si è impegnato nella costante ricerca di soluzioni in grado di seguire gli atenei nel loro cammino di ammodernamento dei metodi di governo di realtà così complesse e articolate; CINECA ha assunto quindi il ruolo di "braccio tecnico operativo" che, attraverso la realizzazione di sofisticati sistemi telematici, consente l'interazione di tutte le componenti del mondo accademico con l'Amministrazione centrale, garantendo al Ministero il costante monitoraggio dei processi ed il coordinamento di tutte le attività.

Il ruolo del Responsabile del sistema di conservazione è ribadito anche nel testo degli accordi di versamento sottoscritti fra Ateneo e Cineca.

In quanto soggetto responsabile, in coerenza con il sistema OAIS, Cineca si occupa delle politiche complessive del Sistema di conservazione e ne determina l'ambito di sviluppo e le competenze.

A tal fine provvede alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del Sistema.

### **1.2.2. Gestione del sistema di conservazione: Organigramma, Struttura organizzativa, Pubblico ufficiale**

Si rimanda al manuale di conservazione del Conservatore, allegato n.5.

## **1.3. Oggetti sottoposti a conservazione**

### **1.3.1. Documenti informatici e loro aggregazione: Serie e relativi Repertori**

Il Sistema di conservazione acquisisce, gestisce, organizza e conserva documenti informatici, in particolare documenti amministrativi informatici, e le loro aggregazioni documentali informatiche sotto forma di fascicoli e serie; ai fini della corretta conservazione nel medio e lungo periodo è indispensabile conoscere la natura di oggetti informativi complessi sia dei documenti che delle loro aggregazioni.

Il documento amministrativo informatico è prodotto e memorizzato su di un supporto elettronico durante lo svolgimento di un'attività di carattere amministrativo e, grazie al Sistema di gestione in cui è stato inserito al momento dell'acquisizione, possiede le opportune caratteristiche di immutabilità, integrità e staticità, come previsto dalla normativa vigente.

Durante la vita nel Sistema di gestione corrente Titulus, il documento è sottoposto a una serie di azioni (es. protocollazione, classificazione, attribuzione al Responsabile del procedimento, attribuzione al fascicolo etc.) che ne determinano la posizione logica all'interno dell'archivio così come l'identità: la particolarità e unicità del documento è caratterizzata proprio dalla specifica funzione che esso riveste nello svolgimento dell'attività del Produttore.

Le caratteristiche proprie del documento vengono tradotte in ambito elettronico in metadati: informazioni connesse al documento che consentono, all'interno del Sistema, l'identificazione, la descrizione, la gestione e la conservazione; la normativa prescrive un pacchetto minimo di metadati da associare al documento informatico immutabile.

In tal senso risulta fondamentale l'appartenenza del documento al fascicolo; la fascicolazione, oltre a essere un obbligo previsto dalla normativa, è il requisito indispensabile per la corretta gestione del documento all'interno del contesto relazionale che ne determina il significato e l'identità. Fascicolare significa esplicitare la posizione logica e fisica del singolo documento all'interno dell'archivio, quindi stabilire esattamente la funzione che il documento svolge; ad esempio, tutti i documenti che fanno parte del medesimo procedimento appartengono allo stesso fascicolo e vanno tenuti insieme nell'ordine cronologico, cosiddetto ordine di sedimentazione, in base al quale si sono formati, e in tal modo si ottiene un fascicolo che contiene la storia del procedimento, e le azioni a cui il documento è soggetto nel corso della propria esistenza, sono strettamente determinate dall'appartenenza al fascicolo.

Il passaggio del documento dal Sistema di gestione Titulus al Sistema di conservazione Conserva, deve consentire il mantenimento delle caratteristiche del documento di immodificabilità, integrità e staticità, così come deve essere mantenuto il legame significativo del documento con il fascicolo al fine di preservare e tramandare per il periodo necessario il valore giuridico probatorio, amministrativo e storico.

Il Codice dell'amministrazione digitale definisce all'art. 1, lettera p) cosa debba intendersi per documento informatico, e al successivo art. 23-ter specifica la particolare categoria di documento informatico rappresentata dal documento amministrativo informatico, ribadendone la natura di informazione primaria e originale; lo stesso art. 23-ter riassume le azioni che è possibile effettuare sul documento amministrativo informatico con uno specifico richiamo alle regole tecniche previste all'art. 71, ossia il DPCM 13 novembre 2014.

Le aggregazioni di documenti informatici o di fascicoli informatici, sono l'insieme definito e qualificato di documenti riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.

Il fascicolo rappresenta, quindi, la prima forma di aggregazione determinata e può essere organizzato raccogliendo documenti diversi per formato, natura, contenuto giuridico, ma prodotti nel corso di una specifica attività; oppure raccogliendo documenti della stessa tipologia o qualità o forma, raggruppati quindi in base a criteri estrinseci, e riguardanti contenuti disomogenei.

In particolare è possibile distinguere tra differenti tipologie di fascicoli: fascicolo di persona, fascicolo di affare, fascicolo di attività, fascicolo procedimentale, fascicolo di fabbricato e fascicolo edilizio.

La distinzione tipologica dei fascicoli deriva dal particolare iter di produzione della documentazione per cui la catena delle azioni che pongono in essere un insieme di documenti determina anche le modalità con cui i documenti vengono organizzati e archiviati, e dà luogo, nel medio e lungo periodo, al cosiddetto processo di sedimentazione.

I fascicoli, così come particolari tipologie di documenti, creano ulteriori aggregazioni documentali definite serie; si tratta di articolazioni interne all'archivio createsi sulla base del processo di sedimentazione reso esplicito dall'applicazione del titolario di classificazione.

Le serie sono funzionali all'individuazione di caratteristiche comuni per documenti o fascicoli, e consentono, di conseguenza, un'efficiente gestione dei dati oltre a rappresentare un elemento indispensabile della struttura dell'archivio; dal punto di vista dei fascicoli, le serie si creano rispettando l'articolazione del titolario di classificazione sulla base del quale i singoli fascicoli vengono classificati e inseriti nel repertorio dei fascicoli. La serie può corrispondere anche al raggruppamento di specifiche tipologie documentali, le quali, quindi, condividono un insieme di caratteristiche omogenee, tradotte in ambito informatico in un set di metadati.

Da un punto di vista normativo, il fascicolo informatico viene introdotto dal Codice dell'amministrazione digitale all'art. 41 in relazione al procedimento amministrativo: "La pubblica

amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati". Nel comma 2ter del suddetto articolo, vengono elencate le indicazioni di cui il fascicolo deve essere provvisto per la corretta identificazione e gestione: "Il fascicolo informatico reca l'indicazione: a) dell'amministrazione titolare del procedimento, che cura la costituzione/gestione dello stesso; b) delle altre amministrazioni partecipanti; c) del Responsabile del procedimento; d) dell'oggetto del procedimento; e) dell'elenco dei documenti contenuti; e-bis) dell'identificativo del fascicolo".

Il successivo art. 44, esplicitando i Requisiti per la gestione e conservazione dei documenti informatici, dichiara che annualmente devono essere trasferiti al Sistema di conservazione "i fascicoli e le serie documentarie anche relative a procedimenti conclusi" (la gestione del fascicolo e delle aggregazioni documentali, viene sostenuta anche dalle regole tecniche di cui al DPCM 13 novembre 2014, all'art. 13 - Formazione dei fascicoli informatici, e all'art 15 - Trasferimento in conservazione).

### **1.3.2. Unità archivistiche e unità documentarie**

Il rapporto tra unità archivistiche e unità documentarie subisce, in ambito informatico, una traslazione rispetto alla tradizione archivistica, e ciò è dovuto a esigenze gestionali legate alla specificità dei supporti con cui vengono veicolate le unità informative in ambito informatico.

L'unità archivistica in ambito analogico è l'unità base costituita dall'insieme di documenti che condividono determinate caratteristiche identificative, risultato di un processo di produzione, che fanno dell'unità, un'aggregazione qualificata e non casuale.

In tal senso, l'unità archivistica è il livello di definizione e descrizione dell'aggregazione documentale oltre il quale non è possibile procedere, ossia i documenti che la costituiscono sono elementi che non possiedono un'identità propria se tolti, ad esempio, dal fascicolo, cioè se decontestualizzati. L'unità archivistica nella maggior parte dei casi corrisponde al fascicolo, quindi un insieme di documenti, ma può corrispondere anche al singolo documento.

In ambito informatico, tale rapporto, benché mantenga il rispetto dei principi archivistici, risulta più complesso, poiché l'unità documentaria diventa a sua volta un contenitore la cui natura è pre-strutturata sulla base della tipologia di informazioni che deve contenere: si articola in documenti principali, allegati, componenti, e le unità informative principali costituiscono il nucleo dell'unità documentaria e determinano la struttura e i metadati di riferimento.

L'Ateneo, in qualità di Produttore, determina la relazione di appartenenza tra i documenti che costituiscono l'unità documentaria e l'unità archivistica, mentre il Conservatore, in un secondo momento, si fa carico di mantenere stabili, consultabili e contestualizzate nel tempo tali informazioni, secondo i parametri definiti nel manuale di conservazione del Conservatore e negli accordi di versamento allegati al presente documento (allegato n.5).

### **1.3.3. Formati**

Il formato è l'insieme di informazioni che determinano la modalità con cui un oggetto digitale viene creato, memorizzato e riprodotto.

Un oggetto digitale è una sequenza di bit fissati con una certa organizzazione fisica su di una memoria; tale contenuto digitale viene memorizzato e definito file.

La possibilità di fruire e utilizzare un file è determinata dalla capacità di rappresentare la sequenza di bit per mezzo di un apposito software che riproduca, sulla base dei codici e delle regole che costituiscono il file stesso, il contenuto e la forma che gli era stata conferita dall'autore.

La corretta conservazione dei documenti nel tempo è determinata anche dalla scelta dei formati idonei a tale scopo, infatti, un problema di cui è necessario tener presente, è costituito dall'obsolescenza dei formati; attualmente la soluzione più sicura, è adottare, fin dal momento della formazione dei contenuti digitali, formati che abbiano le caratteristiche per fornire le maggiori garanzie in termini di conservazione a lungo termine.

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati al presente documento, in cui sono definite le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale delle diverse tipologie documentali, oggetto di conservazione, inclusa la struttura ed i formati utilizzati.

#### **1.3.4. Metadati**

Insieme alla scelta dei formati, la definizione dei metadati è un'operazione fondamentale per l'attività conservativa delle memorie digitali a medio e lungo termine; i metadati vengono esplicitamente citati come oggetti da sottoporre a conservazione, associati ai documenti informatici, ai documenti amministrativi informatici e ai fascicoli informatici o aggregazioni documentali.

I metadati sono informazioni associate ai dati primari creati e trattati: sono a loro volta dati che descrivono, spiegano, localizzano una risorsa informativa rendendo più semplice il suo recupero, utilizzo e gestione. Ad esempio, il riferimento all'autore o alla tipologia di dato, il riferimento temporale alla creazione o registrazione del dato, la classificazione, etc.

Come si può intuire i metadati associati a una risorsa sono potenzialmente infiniti, quindi si è deciso di distinguerli in tre principali categorie:

- Metadati descrittivi, descrivono una risorsa con lo scopo di scoprirla ed identificarla,
- Metadati strutturali, indicano la struttura di oggetti composti, ad esempio i capitoli che assemblano le pagine,
- Metadati amministrativi, descrivono le informazioni volte a favorire la gestione del file (tipo di file, nome del produttore, riferimento temporale etc.).

Il Sistema di conservazione strutturato sul modello OAIS è predisposto per conservare queste differenti tipologie di metadati in luoghi diversi e si avvale di una caratteristica propria dei metadati per cui essi possono far parte del dato stesso o possono essere archiviati come oggetti esterni, e organizzati in gerarchie, ontologie o schemi.

Ad esempio, i dati e i metadati relativi all'oggetto informativo e alle informazioni sulla rappresentazione costituiscono un'unità denominata contenuto informativo e in tale forma viene conservata al fine di assicurare la fruibilità e la comprensibilità nel lungo periodo; i metadati descrittivi, invece, che descrivono e identificano le informazioni archiviate, vengono conservate separatamente in appositi database.

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati al presente documento, in cui sono definite le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale, delle diverse tipologie documentali oggetto di conservazione, inclusi individuazione e gestione dei metadati relativi ai documenti versati nel Sistema di conservazione.

#### **1.3.5. Pacchetto informativo: pacchetto di versamento, di archiviazione, di distribuzione**

Gli oggetti sottoposti a conservazione, siano essi aggregazioni documentali informatiche, documenti informatici, o metadati, sono trasmessi dal Produttore, memorizzati e conservati nel Sistema e distribuiti agli Utenti sotto forma di pacchetti informativi. Il pacchetto informativo, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di Pacchetto di versamento (SIP), Pacchetto di archiviazione (AIP) e Pacchetto di distribuzione (DIP).

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati.

I pacchetti di versamento (SIP) sono concordati per struttura e contenuto con il Produttore e contengono l'oggetto o gli oggetti da conservare. In base alle specifiche esigenze possono contenere una o più unità archivistiche, una o più unità documentarie, eventuali aggiornamenti all'unità documentaria già versata o solo informazioni da associare a un'unità documentaria già

conservata; ogni SIP può generare uno o più Pacchetti di archiviazione così come più SIP possono costituire un unico Pacchetto di archiviazione.

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati.

Il pacchetto di archiviazione (AIP) viene generato dal Sistema a conclusione del processo di acquisizione e presa in carico dei SIP; esso è composto dagli oggetti-dati (file) e dall'indice dell'AIP, un file XML che contiene tutti gli elementi del pacchetto informativo, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal Produttore, sia da quelle generate dal Sistema nel corso del processo di conservazione.

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati.

Il pacchetto di distribuzione (DIP) viene generato dal Sistema a partire dai Pacchetti di archiviazione conservati ed è finalizzato a mettere a disposizione degli utenti, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione.

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati.

## **1.4. Processo di conservazione**

### **1.5.1. Fasi del versamento e logiche di conservazione**

Il processo di conservazione è attivato sulla base degli accordi di versamento stipulati tra l'Ateneo e il Conservatore, in qualità di soggetto che svolge attività di conservazione.

Le procedure per l'attivazione del processo di conservazione sono indicate nell'atto di affidamento dei servizi per l'utilizzo delle soluzioni Cineca e dei servizi di assistenza connessi, che ne costituiscono parte integrante e sono dettagliati negli accordi di versamento.

Il processo di conservazione si basa su di una logica di conservazione caratterizzata dal versamento da parte del Produttore degli oggetti da conservare, cioè documenti informatici e aggregazioni documentali informatiche, secondo la tempistica definita e dettagliata negli accordi di versamento.

### **1.4.2. Acquisizione e presa in carico dei pacchetti di versamento (SIP)**

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati al presente documento.

### **1.4.3. Gestione del pacchetto di archiviazione (AIP)**

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati al presente documento.

### **1.4.4. Gestione del pacchetto di distribuzione (DIP)**

Si rimanda al manuale di conservazione del Conservatore e agli accordi di versamento allegati al presente documento.

### **1.4.5. Monitoraggio e risoluzione delle anomalie**

La segnalazione di un'anomalia o di un incidente può provenire sia dal Produttore (ticket), sia dal gestore del Sistema di conservazione; tali segnalazioni avvengono mediante il sistema di tracciamento attraverso cui sono veicolate le comunicazioni fra i due attori così come la notifica di risoluzione degli stessi in funzione della tipologia di servizio coinvolto.

Il processo di monitoraggio e gestione delle anomalie si applica a tutti gli incidenti e problemi attinenti alle aree:

- Tecnologica (hardware, sistemi operativi e middleware),

- Applicativa,
- Sicurezza delle informazioni,
- Servizi tecnici impianti.

La gestione degli incidenti e anomalie è composta dalle fasi:

- presa in carico e gestione della segnalazione,
- presa in carico e gestione incidente di 1° e 2° livello,
- chiusura incidente,
- monitoraggio incidente.

Si rimanda al manuale di conservazione del Conservatore e relativi disciplinari tecnici allagati al presente documento, in cui sono definite le specifiche operative e le modalità di interazione per la gestione delle anomalie e per il monitoraggio.

## **1.5. Descrizione del sistema di conservazione**

### **1.5.1. Componenti Logiche**

Si rimanda al Manuale di conservazione del Conservatore (allegato n.5).

### **1.5.2. Componenti Fisiche**

Si rimanda al Manuale di conservazione del Conservatore (allegato n.5).

### **1.5.3. Componenti Tecnologiche**

Si rimanda al Manuale di conservazione del Conservatore (allegato n.5).

### **1.5.4. Procedure di gestione del sistema**

Si rimanda al Manuale di conservazione del Conservatore (allegato n.5).

### **1.5.5. Evoluzione del sistema**

Si rimanda al Manuale di conservazione del Conservatore (allegato n.5).

### **1.5.6. Monitoraggio e controlli**

Si rimanda al Manuale di conservazione del Conservatore e agli Accordi di versamento (allegato n.5).

## **1.6. Strategie adottate a garanzia della conservazione**

### **1.6.1. Misure a garanzia della intellegibilità, della leggibilità e della reperibilità nel tempo**

Si rimanda al Manuale di conservazione del Conservatore e agli Accordi di versamento (allegato n.5).

### **1.6.2. Misure a garanzia dell'interoperabilità e della trasferibilità ad altri conservatori**

Si rimanda al Manuale di conservazione del Conservatore e agli Accordi di versamento (allegato n.5).

## **1.7. Trattamento dei dati personali**

Il Responsabile del trattamento dei dati ha il compito di tutela delle informazioni contenute nei documenti da conservare; tale ruolo viene svolto sia dal Produttore che dal Conservatore nelle forme previste dal Codice in materia di protezione dei dati personali.

Per le istruzioni e i compiti ai quali devono attenersi i Responsabili e gli Incaricati del trattamento dei dati dell'Ateneo, per le diverse tipologie di documenti che saranno successivo oggetto di conservazione, si rimanda al Manuale di gestione del protocollo informatico, al Regolamento

per attuazione in materia di protezione dei dati personali e al Regolamento per il trattamento dei dati sensibili e giudiziari in attuazione del D.lgs. 196/2003 emanati dall'Ateneo.

L'Ateneo ha affidato al Consorzio Cineca, dotato di specifica competenza ed esperienza, lo svolgimento del processo di conservazione secondo quanto stabilito nell'atto di affidamento il quale, ai sensi dell'art. 6, comma 8 del DPCM 3 dicembre 2013, assume il ruolo di Responsabile del trattamento dei dati.

Agli effetti del contratto, le parti si sono impegnate a conformarsi alle disposizioni del Codice in materia di protezione dei dati personali e successive modifiche ed integrazioni.

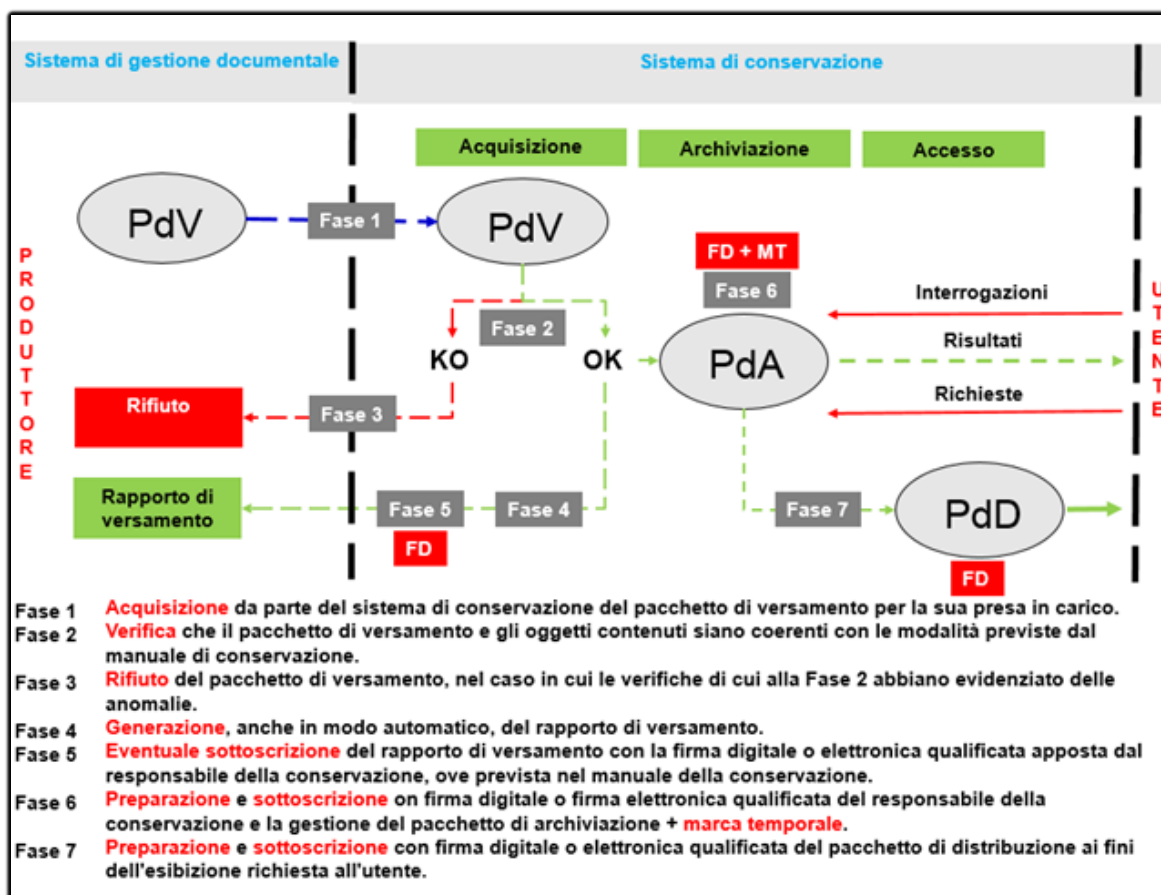
L'Ateneo, titolare dei dati, ai sensi dell'art. 29 del D.lgs. 196/2003, ha nominato il Consorzio Cineca Responsabile esterno del trattamento dei dati personali necessari all'esecuzione di tale atto di affidamento e al compimento degli atti conseguenti, impartendo le istruzioni e individuando i compiti ai quali deve attenersi il Responsabile (i dettagli nell'allegato n.4).

I dati trattati sono sia i *dati personali contenuti nei documenti oggetto di conservazione* che i *dati personali degli utenti del servizio di conservazione*, per consentire l'accesso al Sistema di conservazione.

Le attività di trattamento dei dati personali sono svolte nei limiti strettamente necessari alla realizzazione delle prestazioni richieste, unicamente tramite soggetti debitamente autorizzati (art. 30, D.lgs. 196/2003), secondo i principi di liceità, proporzionalità e correttezza (art. 11, D.lgs. 196/2003), nel rispetto delle misure minime di sicurezza (art. 33, D.lgs. 196/2003 e allegato B, D.lgs. 196/2003).

## 2. Il processo di Conservazione Sostitutiva di UniIT

### 2.1. Descrizione del servizio



#### 2.1.1. Acquisizione dei pacchetti di versamento e presa in carico

L'operazione di versamento consiste nella trasmissione dei documenti da conservare e dei metadati che li specializzano. La ricezione e presa in carico di un pacchetto di

versamento segue uno schema logico di funzionamento che si articola in due fasi distinte: ricezione dell'Indice del Pacchetto di Versamento (IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).

I canali ammessi per la trasmissione sono:

- ✓ interfaccia web,
- ✓ invocazione di metodi tramite web service REST,
- ✓ invio in allegato a una mail PEC,
- ✓ trasferimento via protocollo FTP.

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:

- ✓ l'interfaccia web viaggia su protocollo HTTPS,
- ✓ il web service REST è contattabile tramite protocollo HTTPS,
- ✓ la PEC nativamente garantisce autenticità della provenienza e notifica di consegna in modalità sicura,
- ✓ il server FTP è raggiungibile via SFTP.

Il sistema di conservazione prende in carico un PdV solo dopo che tutte le sue parti (IPdV e relativi documenti) vengono correttamente ricevuti e superano positivamente i relativi controlli; tale operazione viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene inviato o reso disponibile al cliente secondo le modalità previste dall'accordo contrattuale.

I log relativi ai singoli versamenti riportano l'oggetto (indice o documento), il risultato dell'operazione (ok o errore), data e ora e l'utente che ha fatto l'operazione.

### **2.1.2. Ricezione dell'indice del pacchetto di versamento**

L'IPdV è un'evidenza informatica, ovvero un file, che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati. Questi sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

La funzione di ricezione degli indici dei pacchetti di versamento nel sistema di conservazione effettua, per ogni indice, i seguenti controlli:

- ✓ abilitazione alla conservazione da parte del sistema di gestione documentale versante e in particolare dell'utente che effettua il versamento. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- ✓ controllo formale dell'indice versato. In particolare viene verificato che sia un formato XML valido per una delle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- ✓ verifica, tramite l'identificativo univoco contenuto nell'indice, dell'eventuale presenza del PdV già nel sistema;
- ✓ controllo sulla completezza e correttezza formale dei metadati, in relazione alla Classe Documentale rilevata. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- ✓ controllo sulla tipologia di documenti che si vuole versare. Ogni documento deve appartenere ad almeno uno dei formati ammessi dalla tipologia di Classe Documentale. In caso di esito negativo il sistema rifiuta il tentativo di versamento;
- ✓ eventuali controlli supplementari definiti insieme al Cliente. La gestione degli esiti negativi va formalizzata in sede contrattuale.

### **2.1.3. Ricezione documenti associati ad un pacchetto di versamento**

La ricezione dell'IPdV permette al sistema di conservazione di registrare i metadati del PdV e di mettersi in attesa dei documenti per la conservazione del pacchetto; di seguito sono elencati

i controlli già predisposti e che possono essere eseguiti per ciascun formato trattato dal sistema di conservazione di UNI IT:

- ✓ file P7M: viene controllata la validità della firma apposta sul documento e dell'eventuale marca temporale apposta; nel caso di esito negativo il file viene rifiutato e viene restituito un errore. I controlli sulla firma prevedono le seguenti verifiche:
  - controllo di conformità,
  - controllo crittografico,
  - controllo catena Trusted,
  - controllo certificato,
  - controllo CRL;
- ✓ file XML: viene controllata la correttezza formale del file mediante l'uso di un parser software. Se il Cliente fornisce l'xsd, viene applicato in maniera da verificarne l'aderenza;
- ✓ file PDF/A: viene preventivamente controllata la incorruttibilità del file simulandone l'apertura con un opportuno viewer;
- ✓ file EML: vengono controllati gli header del file per verificare che si tratti realmente di una mail. Nel caso di mail PEC viene controllata anche la validità del certificato.

#### **2.1.4. Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico**

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un rapporto di versamento che viene firmato dal Responsabile del servizio di conservazione ed attesta l'avvenuta presa in carico, da parte del sistema di conservazione, dei pacchetti di versamento inviati dal produttore. Esso viene prodotto nel momento in cui tutti gli elementi utili per la conservazione del pacchetto di versamento sono stati consegnati al sistema. Tale rapporto viene anche inviato via PEC, o altro canale certificato, all'indirizzo specificato nella configurazione di sistema.

#### **2.1.5. Preparazione e gestione del pacchetto di archiviazione**

Il pacchetto di archiviazione (PdA) è quello conservato dal sistema di conservazione e possiede un insieme completo di metadati utili alla conservazione a lungo termine. Il pacchetto di archiviazione viene realizzato secondo lo standard di riferimento SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che rappresenta lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

#### **2.1.6. Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione**

Il pacchetto di distribuzione è strutturato nel modello dati come il pacchetto di archiviazione. Considerata la sua destinazione di uso (esibizione), normalmente è un "sottoinsieme" del pacchetto di archiviazione. Un utente autorizzato è in grado di interrogare il sistema per ricevere in uscita uno specifico pacchetto di distribuzione. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

### **2.2. L'Architettura e l'infrastruttura**

#### **2.2.1. Infrastruttura Informatica**

I Data Center dal quale sono erogati i servizi si trovano sul territorio nazionale e sono conformi ai requisiti della normativa. Nelle due strutture a disposizione viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

### 2.2.2. Caratteristiche generali della soluzione di conservazione

La soluzione presenta le seguenti caratteristiche peculiari:

- architettura di produzione, implementata su infrastruttura virtuale e storage dedicati, predisposta totalmente ridondata (HA) presso il Data Center che ospita la soluzione e che rispetta le caratteristiche proprie della certificazione Tier IV dell'Uptime Institute,
- architettura secondaria predisposta per consentire la doppia scrittura del dato, effettuata applicativamente, e la replica sincrona storage based della piattaforma virtuale, inclusi i DB documentali e di gestione, situata presso il Data Center secondario.

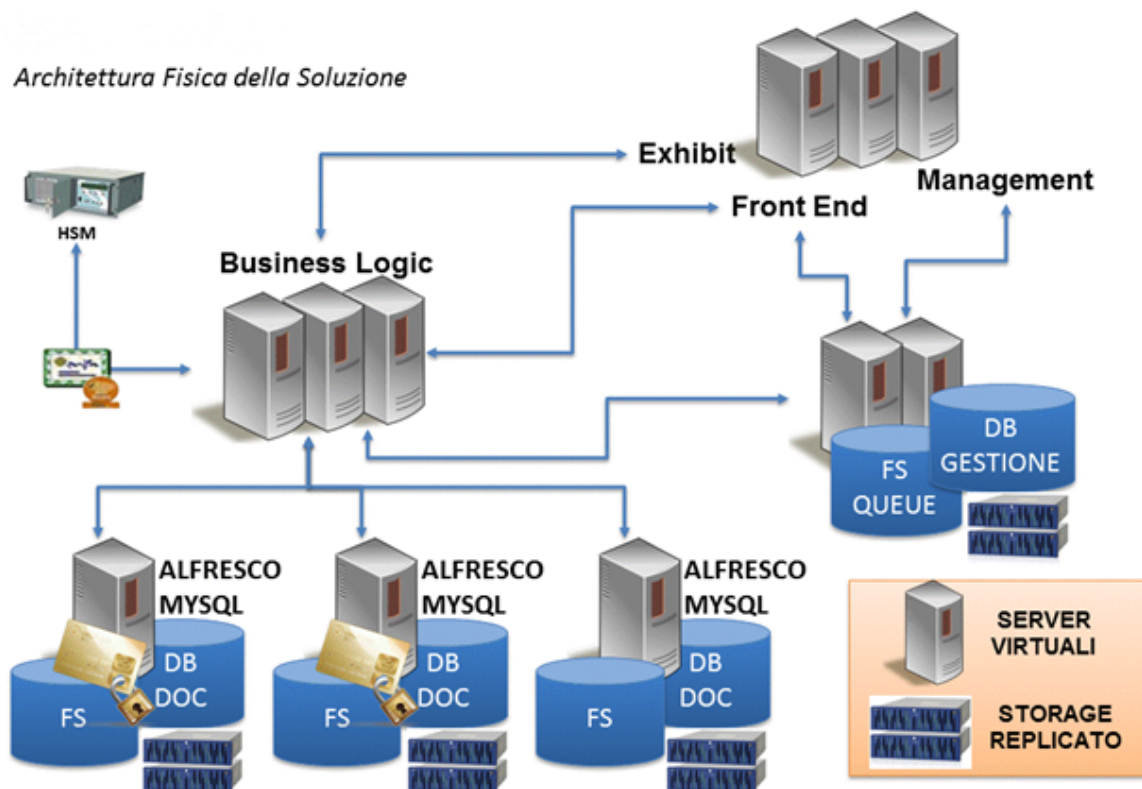
### 2.2.3. Affidabilità - Totale ridondanza ai guasti HW

- Funzionalità di HA (High availability) implementata dall'architettura virtuale.
- Almeno due moduli con il medesimo ruolo posizionati su server fisici separati.
- DBMS in configurazione Master-Master.
- Sistemi documentali duplicati "gemelli".
- Doppia scrittura dei documenti.
- Utilizzo di sistemi di firma e marca ad alte prestazioni in HA.

Architettura scalabile

- Nodi di Front-End ed Application multipli e contemporaneamente attivi.
- Storage di livello Enterprise ad alte prestazioni per piattaforma VMware e componenti Database.
- Funzionalità di replica.

### 2.2.4. Architettura fisica



## 2.3. Certificazioni UniIT

### 2.3.1. ISO IEC 20000-1:2011

|                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |                                                                                                                                                                                                                                                                                               |              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <br>ISTITUTO DI CERTIFICAZIONE DELLA QUALITÀ<br>www.certiquality.it                                                                                                                                                                                                                                                                                             |            | <br>CISQ is a member of<br>IONet<br>www.ionet-certification.com                                                                                                                                            |              |
| CERTIFICATO n. 20745<br>CERTIFICATE No 20745                                                                                                                                                                                                                                                                                                                                                                                                     |            | IONet, the association of the world's first class certification bodies, is the largest provider of management system Certification in the world.<br>IONet is composed of more than 30 bodies and counts over 150 subsidiaries all over the globe.                                             |              |
| SI CERTIFICA CHE L'ORGANIZZAZIONE<br>WE HEREBY CERTIFY THAT THE ORGANIZATION                                                                                                                                                                                                                                                                                                                                                                     |            |                                                                                                                                                                                                                                                                                               |              |
| <b>UNI IT S.r.l.</b>                                                                                                                                                                                                                                                                                                                                                                                                                             |            |                                                                                                                                                                                                                                                                                               |              |
| IT - 38122 TRENTO (TN) - VIA G. GALILEI 1                                                                                                                                                                                                                                                                                                                                                                                                        |            |                                                                                                                                                                                                                                                                                               |              |
| NELLE SEGUENTI UNITÀ OPERATIVE / IN THE FOLLOWING OPERATIVE UNITS<br>IT - 38122 TRENTO (TN) - VIA G. GALILEI 1                                                                                                                                                                                                                                                                                                                                   |            |                                                                                                                                                                                                                                                                                               |              |
| HA IMPLEMENTATO E MANTIENE UN SISTEMA DI GESTIONE QUALITÀ / SHE HAS IMPLEMENTED AND MAINTAINS A QUALITY MANAGEMENT SYSTEM WHICH COMPLIES WITH THE FOLLOWING STANDARD                                                                                                                                                                                                                                                                             |            |                                                                                                                                                                                                                                                                                               |              |
| <b>ISO IEC 20000-1:2011</b>                                                                                                                                                                                                                                                                                                                                                                                                                      |            |                                                                                                                                                                                                                                                                                               |              |
| PER LE SEGUENTI ATTIVITÀ / FOR THE FOLLOWING ACTIVITIES                                                                                                                                                                                                                                                                                                                                                                                          |            | SETTORE<br>CODE                                                                                                                                                                                                                                                                               | <b>EA 33</b> |
| Erogazione di servizi informatici a progetto e a listino verso la Pubblica Amministrazione e verso le banche, con particolare riferimento all'ordinativo informatico e alla conservazione di documenti.<br><i>Delivery of IT services (both on a project basis and a catalog basis) for the Public Administration and the banks and financial institutions, with a special regard to the processing orders and validated documents' storage.</i> |            |                                                                                                                                                                                                                                                                                               |              |
| IL PRESENTE CERTIFICATO È SOGGETTO AL RISPETTO DEL REGOLAMENTO PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE<br>THE USE AND THE VALIDITY OF THE CERTIFICATE SHALL SATISFY THE REQUIREMENTS OF THE RULES FOR THE CERTIFICATION OF MANAGEMENT SYSTEMS                                                                                                                                                                                              |            |                                                                                                                                                                                                                                                                                               |              |
| PRIMA EMISSIONE<br>FIRST ISSUE                                                                                                                                                                                                                                                                                                                                                                                                                   | 16/10/2014 | <br>CERTIQUALITY S.r.l. - IL DIRETTORE GENERALE<br>Via G. Galilei 4 - 20123 MILANO (MI) - ITALY                                                                                                            |              |
| EMISSIONE CORRENTE<br>CURRENT ISSUE                                                                                                                                                                                                                                                                                                                                                                                                              | 16/10/2014 |                                                                                                                                                                                                                                                                                               |              |
| DATA SCADENZA<br>EXPIRY DATE                                                                                                                                                                                                                                                                                                                                                                                                                     | 15/10/2017 |                                                                                                                                                                                                                                                                                               |              |
| MOD. CERT. 01/18/03                                                                                                                                                                                                                                                                                                                                                                                                                              |            | Per informazioni sulla validità del certificato, visitate il sito <a href="http://www.ionet.it">www.ionet.it</a><br>For information concerning the validity of the certificate, you can visit the site <a href="http://www.ionet.it">www.ionet.it</a>                                         |              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            | La validità del presente certificato è subordinata a sorveglianza periodica annuale ed al riesame completo del Sistema di Gestione con periodicità triennale.<br>The validity of the certificate depends on annual audit and on a complete review every three years of the Management System. |              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            | <br>www.cisq.com                                                                                                                                                                                         |              |

### 2.3.2. UNI CEI ISO/IEC 27001:2014



ISTITUTO DI CERTIFICAZIONE DELLA QUALITÀ  
www.certiquality.it

CERTIFICATO n. **21125**  
CERTIFICATE No

SI CERTIFICA CHE L'ORGANIZZAZIONE  
WE HEREBY CERTIFY THAT THE ORGANIZATION

**UNI IT S.r.l.**

IT - 38122 TRENTO (TN) - VIA G. GALILEI 1

NELLE SEGUENTI UNITÀ OPERATIVE / IN THE FOLLOWING OPERATIVE UNITS

IT - 38122 TRENTO (TN) - VIA G. GALILEI 1

HAI ATTUATO E MANTIENE UN SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI CHE È CONFORME ALLA NORMA  
HAS IMPLEMENTED AND MAINTAINS AN INFORMATION SECURITY MANAGEMENT SYSTEM WHICH COMPLIES WITH THE FOLLOWING STANDARD

**UNI CEI ISO/IEC 27001:2014**

PER LE SEGUENTI ATTIVITÀ / FOR THE FOLLOWING ACTIVITIES SETTORE CODE **EA 33**

Commercializzazione ed erogazione di servizi informatici a progetto e a listino verso soggetti pubblici e privati inerenti la conservazione dei documenti.

Certificato emesso in accordo con la versione della dichiarazione di applicabilità del 09/07/2015.  
Marketing and delivery of IT services, both on a project basis and a catalog basis, for public and private customers, regarding to digitizing and storage of documents.

Certificate issued in compliance with the version of statement of applicability of 09/07/2015.

CERTIFICATO EMESSE IN ACCORDO CON L'ULTIMA VERSIONE DELLA DICHIARAZIONE DELL'APPLICABILITÀ  
CERTIFICATE ISSUED IN COMPLIANCE WITH THE LAST VERSION OF THE STATEMENT OF APPLICABILITY  
IL PRESENTE CERTIFICATO È SUGLIATO AL RISPETTO DEL REGOLAMENTO PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE  
THE USE AND THE VALIDITY OF THE CERTIFICATE SHALL SATISFY THE REQUIREMENTS OF THE RULES FOR THE CERTIFICATION OF MANAGEMENT SYSTEMS

PRIMA EMISSIONE  
FIRST ISSUE

01/08/2014

EMISSIONE CORRENTE  
CURRENT ISSUE

28/07/2015

DATA SCADENZA  
EXPIRY DATE

31/07/2017

CERTIQUALITY S.r.l. - IL DIRETTORE GENERALE

Via G. Galilei 1 - 38122 TRENTO (TN) - ITALY

CISQ è la Federazione Italiana di  
Organismi di Certificazione dei  
sistemi di gestione aziendale.

CISQ is the Italian Federation  
of management system  
Certification Bodies.



CO. ED. 02/201110

SGQ N° 008A SSC N° 008B  
SGA N° 001D SAF N° 003H  
SGR N° 002F SSI N° 007G  
PSM N° 006I SCE N° 001H

Membro dell'accordo di Riconoscimento EA, IAF e ILAC  
Signatory of EA, IAF and ILAC Mutual Recognition Agreement

Per informazioni sulla validità del  
certificato, visitare il sito  
www.certiquality.it

For information concerning the validity  
of the certificate, visit our web site  
www.certiquality.it

La validità del presente certificato è  
subordinata a sorveglianza periodica  
annuale ed al riesame completo del  
Sistema di Gestione con periodicità  
triennale.

The validity of this certificate depends  
on annual audit and on a complete  
review every three years of the  
Management System.



www.cisq.com

## 2.3.3. UNI EN ISO 9001:2015



CERTIFICATO n. **19187**  
 CERTIFICATE No

SI CERTIFICA CHE L'ORGANIZZAZIONE  
 WE HEREBY CERTIFY THAT THE ORGANIZATION

**UNI IT S.r.l.**

IT - 38122 TRENTO (TN) - VIA G. GALILEI 1

NELLE SEGUENTI UNITA' OPERATIVE / IN THE FOLLOWING OPERATIVE UNITS

IT - 38122 TRENTO (TN) - VIA G. GALILEI 1

HA ATTUATO E MANTIENE UN SISTEMA DI GESTIONE QUALITA' CHE E' CONFORME ALLA NORMA  
 HAS IMPLEMENTED AND MAINTAINS A QUALITY MANAGEMENT SYSTEM WHICH COMPLIES WITH THE FOLLOWING STANDARD

**UNI EN ISO 9001:2015**

PER LE SEGUENTI ATTIVITA' / FOR THE FOLLOWING ACTIVITIES SETTORE CODE **IAF 33, 32**

Sviluppo, commercializzazione ed erogazione di servizi informatici a progetto e a listino verso la Pubblica Amministrazione e verso le banche, con particolare riferimento all'ordinativo informatico e alla conservazione sostitutiva.  
*Development, marketing and delivery of IT services (both on a project basis and a catalog basis) for the Public Administration and the banks and financial institutions, with a special regard to the processing orders and validated document digitizing and storage.*

RIFERIRSI AL MANUALE DI GESTIONE QUALITA' PER L'APPLICABILITA' DEI REQUISITI DELLA NORMA  
 REFER TO MANAGEMENT SYSTEM MANUAL FOR DETAILS OF APPLICATION TO STANDARD REQUIREMENTS

IL PRESENTE CERTIFICATO E' SOGGETTO AL RISPETTO DEL REGOLAMENTO PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE  
 THE USE AND THE VALIDITY OF THE CERTIFICATE SHALL SATISFY THE REQUIREMENTS OF THE RULES FOR THE CERTIFICATION OF MANAGEMENT SYSTEMS

PRIMA EMISSIONE **24/10/2013**  
 FIRST ISSUE  
 EMISSIONE CORRENTE **24/10/2016**  
 CURRENT ISSUE  
 DATA SCADENZA **23/10/2019**  
 EXPIRY DATE

*Emilio Toffi*  
 CERTIQUALITY S.r.l. - IL PRESIDENTE  
 Via G. Galilei 4 - 20123 MILANO (MI) - ITALY



001 ED 03 010616

Member of the Accord of Mutual Recognition EA, IAF and ILAC  
 Signatory of EA, IAF and ILAC Mutual Recognition Agreements

CISQ is a member of



IO Net, the association of the world's first class certification bodies, is the largest provider of management System Certification in the world.  
 never incorporated errors than jobs done and since over 150 subsidiaries all over the globe.

For information concerning the validity of the certificate, you can visit the site [www.certifiqual.it](http://www.certifiqual.it)

The validity of the certificate depends on annual audit and on a complete review every three years of the Management System.



[www.cisq.com](http://www.cisq.com)

CISQ è la Federazione Italiana di Organismi di Certificazione dei sistemi di gestione aziendale.  
 CISQ is the Italian Federation of management system Certification Bodies.



THE INTERNATIONAL CERTIFICATION NETWORK

# CERTIFICATE

IQNet and its partner  
**CISQ/CERTIQUALITY S.r.l.**

**UNI IT S.r.l.**

IT - 38122 TRENTO (TN) - VIA G. GALILEI 1

has implemented and maintains a

**Quality Management System**

which fulfills the requirements of the following standard

**ISO 9001:2015**

for the following activities

Code **IAF 33, 32**

Development, marketing and delivery of IT services (both on a project basis and a catalog basis) for the Public Administration and the banks and financial institutions, with a special regard to the processing orders and validated document digitizing and storage.

in the following operative units

IT - 38122 TRENTO (TN) - VIA G. GALILEI 1

Issued on: **2016-10-24**

Certified since: **2013-10-24**

Expire on: **2019-10-23**

Registration number: **IT-78043**



Michael Drechsel

President of IQNET



Ing. Claudio Provetti

President of CISQ

**IQNet Partners\*:**

AENOR Spain AFNOR Certification France AIB-Vincotte International Belgium APCER Portugal CCC Cyprus  
CISO Italy CQC China CQM China CQS Czech Republic Cro Cert Croatia DQS Holding GmbH Germany  
FCAV Brazil FCNDONORMA Venezuela ICONTEC Colombia IMNC Mexico Inspecta Certification Finland INTECO Costa Rica  
IRAM Argentina JQA Japan KFQ Korea MIRTEC Greece MSZT Hungary Nemko AS Norway NSAI Ireland PCBC Poland  
Qualiity Austria Austria RR Russia SIGE Mexico SII Israel SIQ Slovenia SIRIM QAS International Malaysia  
SQS Switzerland SRAC Romania TEST St Petersburg Russia TSE Turkey YUQS Serbia  
IQNet is represented in the USA by AFNOR Certification, CISQ, DQS Holding GmbH and NSAI Inc.

\* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under [www.iqnet-certification.com](http://www.iqnet-certification.com)

**ALLEGATO 1**

## **Normativa di riferimento**

Decreto Legislativo 26 agosto 2016, n. 179, *Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.*

Decreto Legislativo 12 maggio 2016, n. 90, *Completamento della riforma della struttura del bilancio dello Stato, in attuazione dell'art. 40, comma 1, della legge 31 dicembre 2009, n. 196.*

Direttiva dell'Unione Europea (UE) n. 680/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.*

Regolamento dell'Unione Europea (UE) n. 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*

Decreto Legislativo 7 gennaio 2016, n. 2, *Attuazione della direttiva 2014/60/UE relativa alla restituzione dei beni culturali usciti illecitamente dal territorio di uno Stato membro e che modifica il regolamento (UE) n. 1024/2012.*

Risoluzione dell'Agenzia delle Entrate 25 settembre 2015, n.81/E, Interpello art. 11, legge 27 luglio 2000, n. 212, *Comunicazione del luogo di conservazione in modalità elettronica dei documenti rilevanti ai fini tributari, art. 5 D.M. 17 giugno 2014.*

Decreto Legislativo 5 agosto 2015, n. 127, *Trasmissione telematica delle operazioni IVA e di controllo delle cessioni di beni effettuate attraverso distributori automatici, in attuazione dell'art. 9, comma 1, lettere d) e g), della legge 11 marzo 2014, n. 23.*

Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli artt. 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

Regolamento dell'Unione Europea (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.*

Circolare dell'Agenzia delle Entrate 24 giugno 2014, n. 18/E, *IVA. Ulteriori istruzioni in tema di fatturazione.*

Decreto del Ministro dell'Economia e delle Finanze 17 giugno 2014, *Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - art. 21, comma 5, del decreto legislativo n. 82/2005.*

Circolare dell'Agenzia per l'Italia Digitale - AgID 10 aprile 2014, n. 65, *Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'art. 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.*

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, *Regole tecniche in materia di Sistema di conservazione ai sensi degli artt. 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

Decreto del Ministro dell'Economia e delle Finanze 3 aprile 2013, n. 55, *Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.*

Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.*

Decreto Legge 22 giugno 2012, n. 83, convertito con Legge 7 agosto 2012, n. 134, *Misure urgenti per la crescita del Paese.*

Decreto Legislativo 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale.*

Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, *Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3.*

Decreto del Ministro dell'Economia e delle Finanze 23 gennaio 2004, *Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto.*

Decreto Legislativo 22 gennaio 2004, n. 42, *Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137.*

Decreto Legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali.*

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.*

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, *Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.*

Legge 7 agosto 1990, n. 241, *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.*

### **Istruzioni, linee guida e documentazione informativa**

Istruzioni dell'Agenzia per l'Italia Digitale – AgID marzo 2015, *Produzione e conservazione del registro giornaliero di protocollo.*

Linee guida dell'Agenzia per l'Italia Digitale – AgID dicembre 2015, *Linee guida sulla conservazione dei documenti informatici.*

Linee guida dell'Agenzia per l'Italia Digitale – AgID 26 aprile 2016, *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni – Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015).*

European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016.*

European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on the right to data portability Adopted on 13 December 2016.*

Linee guida del Garante per la protezione dei dati personali 2 marzo 2011, n. 088 del registro dei provvedimenti, *Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.*

Linee guida del Garante per la protezione dei dati personali, 4 aprile 2013, n. 161 del registro dei provvedimenti,

*Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach).*

Linee guida del Garante per la protezione dei dati personali, 15 maggio 2014 n. 243 del registro dei provvedimenti, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati.*

Scheda informativa del Garante per la protezione dei dati personali, 17 marzo 2016, *Scheda informativa sulla figura del Responsabile della protezione dei dati personali (Data Protection Officer).*

Guida informativa del Garante per la protezione dei dati personali, giugno 2016, *Prima guida informativa al Regolamento europeo 2016/679 in materia di protezione dei dati personali.*

### **Standard di riferimento: metadati, archivi digitali, depositi di conservazione**

Per la conservazione digitale l'importanza degli standard nasce dal problema dell'interoperabilità e questo per diverse ragioni:

- l'utilizzo di una risorsa digitale presuppone la capacità di decodificarne e restituirne correttamente il contenuto ed è necessario poter interpretare correttamente i metadati associati alla risorsa,
- i soggetti produttori e i soggetti beneficiari agiscono a distanza di spazio e di tempo, e dunque non è possibile assumere che possano fare affidamento sulle stesse risorse tecnologiche (sistemi di elaborazione ed applicazioni software),
- durante il processo di conservazione, la risorsa digitale passa potenzialmente attraverso diversi cambi di custodia, viene cioè scambiata tra diversi Sistemi di conservazione e affinché tali Sistemi possano colloquiare correttamente occorre che la loro struttura ed il loro modo di operare osservi regole precise, note e condivise.

Se poi ci si pone il problema di verificare e certificare la qualità del processo di conservazione, ciò può concretamente essere fatto solo con riferimento a schemi architetture e organizzativi noti e concordati: gli standard. Essi descrivono in dettaglio, a seconda dei casi, il formato delle risorse, la struttura e il significato dei metadati associati alle risorse, l'organizzazione dei sistemi di archiviazione e conservazione e le modalità con cui si scambiano pacchetti informativi.

Gli standard vengono emessi da organismi nazionali od internazionali di riconosciuta autorevolezza, in primis l'ISO (International Standard Organization), al termine di un iter di approvazione spesso lungo, complesso e rigoroso. Ed è appunto ciò che conferisce loro il ruolo di insostituibile punto di riferimento.

Raggruppamento dei principali standard di interesse nel settore della conservazione digitale:

#### **Metadati**

- ✓ LoC-DLF METS: 2001 – *Metadata Encoding and Transmission Standard.*
- ✓ NLZ Preservation metadata: 2003 – *National Library of New Zealand Metadata -Standards Framework – Metadata Implementation Schema.*
- ✓ OCLC-RLG PREMIS: 2005/2008 – *PREMIS Data Dictionary for Preservation Metadata.*
- ✓ ISO 23081-1/3:2011 – *Information and documentation – Metadata for records.*

#### **Archivi digitali**

- ✓ ISO 15489-1/2: 2001 – *Information and documentation – Records management.*
- ✓ DoD 5015.02-STD: 2007 – *Design Criteria Standard for Electronic Records Management Software Applications.*
- ✓ EU-DML Forum MoReq2: 2008 – *Model Requirements for the Management of Electronic*

#### *Records.*

- ✓ ICA guidelines: 2008 – *Principles and Functional Requirements for Records in Electronic Office Environments.*
- ✓ ISO 16175-1/3: 2010 – *Information and documentation – Principles and functional requirements for records in electronic office environments.*
- ✓ EU-DML Forum MoReq2010: 2011 – *Modular Requirements for Records Systems.*

#### **Depositi di conservazione**

- ✓ ISO/TR 18492: 2005 – *Long-term preservation of electronic document-based information.*
- ✓ ISO 14721:2005/2012 – *Space data and information transfer systems – Open archival information system (OAIS) Reference model.*
- ✓ ISO 16363:2012 – *Audit and certification of trustworthy digital repositories.*
- ✓ ISO 16919:2014 – *Space data and information transfer systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories.*

## **Allegato 2**

### UNIVERSITA' PER STRANIERI DI PERUGIA

| <u>AREA ORGANIZZATIVA OMOGENEA</u> | <u>UNITA' ORGANIZZATIVE RESPONSABILI ( AOO )</u><br>(UOR) |
|------------------------------------|-----------------------------------------------------------|
|------------------------------------|-----------------------------------------------------------|

#### Amministrazione Centrale

Centro Valutazione Certificazione Linguistica  
U.O. Sviluppo e Promozione Convenzioni Centri di Esame  
Centro WARREDOC  
Dipartimento di Scienze Umane e Sociali  
U.S. Gestione Amministrativo-Contabile  
Servizio Segreteria D.G. e Protocollo  
Servizio Segreteria Rettore  
Servizio Programmazione, Qualità e Valutazione

Servizio Relazioni Internazionali, Erasmus e Mobilità

Servizio Organi Collegiali

Servizio Ricerca e Alta Formazione

Servizio Comunicazione e Ufficio Stampa

U.O. Progetti

U.O. Qualità

### Area Servizi agli Studenti

Servizio Orientamento

Servizio Biblioteca

### Area Affari Legali e Contratti

Servizio Contenzioso

Servizio Contratti, Appalti

### Area Segreterie

Servizio Segreteria Corsi di Laurea e Didattica

Servizio Segreteria Studenti Stranieri

U.O. Attività Ricreative ed ex Alunni

U.S. Welcome

### Area Risorse Umane

Servizio Personale T.A.

Servizio Personale Docente

U.O. Formazione

### Area Risorse Finanziarie

Servizio Bilancio e Contabilità

Servizio Trattamenti Economici

U.O. Fiscale

U.O. Pensioni

### Area Patrimonio

Servizio Acquisti e Manutenzione

Servizio Accoglienza e Patrimonio

### Area Servizi Generali

Servizio Supporto RPCT

Servizio Edilizia

Servizio Infrastrutture Informatiche

Servizio Supporto Tecnico

Servizio Sistemi Informativi

### ALLEGATO 3

#### **Nomina e Compiti ai quali deve attenersi il Responsabile esterno al trattamento dei dati personali, ed Elenco delle tipologie documentarie soggette a conservazione, per quanto concerne CINECA**

Il consorzio Cineca, in qualità di Responsabile esterno del trattamento di dati personali per conto di dell'Università per Stranieri di Perugia, ente produttore, ai sensi dell'art. 2 dell'atto di affidamento n. 16030401 Rep. n. 11/2016 del 22 dicembre 2016 e relativi allegati che ne costituiscono parte integrante, si impegna ad attenersi alle istruzioni impartite dal Titolare e svolgere i compiti previsti dal D.lgs. n. 196/2003.

In particolare, i dati personali e/o sensibili e/o giudiziari della banca dati Conserva, del cui trattamento Cineca è con tale atto nominato Responsabile, sono relativi a dati anagrafici, di carriera, di salute, economici del personale, degli studenti e di soggetti esterni che intrattengono con l'Ateneo a qualunque titolo rapporti di natura economica, finanziaria, commerciale, istituzionale o di collaborazione scientifica; tali dati sono versati al del sistema di conservazione attraverso il sistema di gestione documentale Titulus mediante gli accordi di versamento siglati tra Cineca e l'Ateneo, e ai quali si rimanda.

La banca dati in questione è localizzata al Cineca.

L'ambito di designazione di Cineca a Responsabile del trattamento è individuato nei trattamenti effettuati nello svolgimento delle attività, connesse alla gestione del sistema di conservazione Conserva:

- a) Conservazione e manutenzione del sistema informativo e della banca dati Conserva e specificamente:
  - installazione e gestione delle componenti software di infrastruttura (ivi incluso il database) compresi aggiornamenti del sistema informativo e, ove necessario migrazione e adeguamento delle basi dati,
  - *tuning* del sistema (ivi incluso il database) e dell'infrastruttura,
  - monitoraggio del servizio e dei componenti del sistema (ivi incluso il database),
  - supporto, *troubleshooting*, *problem determination* e *problem solving* sul malfunzionamento del servizio dovuto a cause infrastrutturali del Data Center del CINECA,
  - attività di *disaster recovery*,
  - attività di *database administration* (salvataggio e ripristino dei dati, *import* ed *export* dei dati, aggiornamento della base dati connessa ad eventuale aggiornamenti di componenti software, *db fixing*);
- b) Creazione in Cineca di ambienti di test mediante copia (parziale o totale) delle basi dati utilizzate dal sistema Conserva, da utilizzarsi esclusivamente per la diagnostica degli errori, per l'esecuzione dei piani di test funzionali per la validazione di nuove versioni del software, per le verifiche di carico e performance dell'intero sistema. Le copie devono essere distrutte una volta terminate le attività;
- c) Accesso alla banca dati Conserva dell'Ateneo, in modo procedurale e non procedurale, finalizzato alla verifica delle segnalazioni di anomalie collegate al versamento dei documenti nel sistema di conservazione o a problematiche connesse con il sistema di conservazione e

il recupero dei documenti. Il servizio comporta la registrazione delle segnalazioni nel sistema di *Trouble Ticketing* di Cineca.

Il trattamento dei dati, in modo procedurale e non procedurale, da parte di Cineca, è inoltre consentito nello svolgimento di ulteriori attività in favore dell'Ateneo, qualora dalla stessa richieste espressamente e purché strettamente correlate all'uso del *software*, finalizzate a:

- addestramento del personale dell'Ateneo,
- consulenza applicativa, ivi incluso l'adeguamento della configurazione del sistema Conserva a mutate esigenze dell'Ateneo,
- sviluppo e/o attivazione di funzionalità specifiche richieste dall'Ateneo, che possono anche richiedere caricamento massivo di dati,
- estrazioni selettive di documenti, nel rispetto delle indicazioni fornite dal responsabile della conservazione dell'Ateneo richiedente il servizio,
- importazione di pacchetti di archiviazione o lotti di versamento provenienti da altri sistemi di conservazione,
- esportazione pacchetti di archiviazione per il trasferimento ad altri sistemi di conservazione.

Tutte le attività sopra elencate potranno essere svolte da Cineca anche per via telematica. In questo caso l'Ateneo fornirà ad esso tutte le informazioni necessarie per il collegamento, nel pieno rispetto delle norme predisposte dall'Ateneo e dal Responsabile stesso in materia di sicurezza della trasmissione dati.

Il Responsabile provvede, per quanto di sua competenza, con specifico riferimento a quanto disposto dagli artt. 33, 34, 35 e 36 del Decreto Legislativo 30 giugno 2003, n. 196 e come previsto all'art. 20 e nell'allegato 1 del Regolamento di attuazione dello stesso, emanato con D.R. n. 7445 dell'11 gennaio 2005 ed entrato in vigore il 27 gennaio 2005 pubblicato sul sito di Ateneo, ad adempiere all'incarico adottando idonee e preventive misure di sicurezza al fine di prevenire:

- i rischi di distruzione, perdita anche accidentale di dati o danneggiamento delle banche dati o dei locali ove esse sono custodite,
- l'accesso non autorizzato ai dati stessi,
- modalità di trattamento dei dati non consentite rispetto alla legge,
- modalità di trattamento dei dati non conformi rispetto alle finalità della raccolta.

Il Titolare affida pertanto a Cineca ogni incombenza connessa all'esecuzione dell'incarico di Responsabile conferito e necessaria/opportuna per l'esercizio dei compiti specificamente affidati, attribuendogli il potere di adottare tutte le iniziative e gli interventi idonei a garantire il corretto esperimento della funzione affidata.

Quanto sopra fermo restando l'obbligo a carico di Cineca di operare secondo le istruzioni generali impartite dal Titolare e di fornire al medesimo tutte le informazioni necessarie per consentire l'attuazione di adeguate verifiche periodiche.

In base a tale nomina a Responsabile del Trattamento, il Cineca dovrà in particolare curare i seguenti adempimenti, ciascuno all'interno della propria struttura:

- **nominare** con propri atti scritti gli incaricati del trattamento e gli eventuali amministratori di sistema, di *database* e di *software* complesso e fornire loro dettagliate istruzioni operative. Tale designazione deve individuare puntualmente l'ambito del trattamento consentito (banche dati, operazioni effettuabili e durata dell'incarico). Gli incaricati devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del Titolare o del Responsabile sotto la cui diretta autorità operano. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, devono essere individuati dal Responsabile e configurati dall'Amministratore di sistema anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Per quanto attiene al trattamento dei dati sensibili e/o giudiziari, la lista degli incaricati può

essere redatta dai Responsabili del trattamento dei dati anche per classi omogenee di incarico e dei relativi profili di autorizzazione;

- **sovrintendere e vigilare** sull'attività degli incaricati e sull'attuazione delle istruzioni impartite, nonché, in generale, sul rispetto della normativa in materia di tutela dei dati personali, provvedendo personalmente alla formazione degli incaricati medesimi in materia di protezione dei dati personali;
- **verificare, almeno annualmente**, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione assegnati agli incaricati del trattamento. Il Responsabile deve verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione anche in caso di: cambio di ruolo (variazione dei privilegi); dimissioni/licenziamento di un incaricato del trattamento (revoca del profilo); assenza prolungata dal luogo di lavoro (sospensione del profilo).

Il Responsabile deve darne immediata comunicazione all'Amministratore di sistema che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione.

- **conservare e mantenere aggiornato**, in base a quanto prescritto nel provvedimento del 27/11/2008 del Garante (*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni della funzione di amministratore di sistema*) e successive modifiche, gli estremi identificativi (nome, cognome, area organizzativa di appartenenza) delle persone fisiche preposte quali amministratori di sistema/database /*software* complesso;
- **comunicare** al Titolare i nominativi degli incaricati e degli amministratori di sistema/database/*software* complesso;
- **assicurare** la predisposizione e aggiornamento di un sistema di sicurezza dei dati, in conformità con le misure minime prescritte nel D.lgs. 196/2003 e successivi aggiornamenti;
- **attestare** l'adozione di misure minime di sicurezza, la conformità degli interventi alle disposizioni di cui alla misura 25 dell'Allegato B del D.lgs. n. 196/2003 e trasmettere tale attestazione al responsabile delle operazioni di trattamento dei dati personali e all'amministratore di sistema;
- **dare riscontro oralmente**, anche tramite propri incaricati, alle richieste dell'interessato di cui ai commi 1 e 2 dell'art. 7 del D.lgs. n. 196/2003, con le modalità indicate nell'art. 9 del citato decreto;
- **trasmettere**, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e ss. del D.lgs. n. 196/2003, che necessitino di riscontro scritto, al Responsabile della conservazione, referente dell'Ente produttore nominato, per consentire allo stesso di dare riscontro all'interessato nei termini stabiliti dal suddetto decreto; fornire inoltre al referente la massima assistenza, necessaria per soddisfare tali richieste, nell'ambito dell'incarico affidatogli;
- **dare piena collaborazione** al Titolare nell'esecuzione di verifiche periodiche.

In relazione allo specifico incarico di detenzione della banca dati del servizio Conserva e di eventuali copie di essa, Cineca, in qualità di amministratore di sistema, deve inoltre:

- **adottare**, per i sistemi e data base che detiene, sistemi idonei alla registrazione degli accessi logici agli stessi da parte degli amministratori di sistema/database/*software* complesso, in base a quanto prescritto nel citato provvedimento del 27/11/2008 del Garante e successive modifiche,
- **verificare** l'operato degli amministratori di sistema/database/*software* complesso nominati con una cadenza almeno annuale, al fine di controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali e/o sensibili e/o giudiziari.

In base a tale nomina a Responsabile esterno del Trattamento, il Cineca:

- si impegna a non divulgare, diffondere, trasmettere e comunicare i dati/documenti informatici di proprietà del Titolare del trattamento, nella piena consapevolezza che i dati/documenti rimarranno sempre e comunque di proprietà esclusiva dello stesso Titolare del trattamento, e pertanto non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti;
- si impegna, previa restituzione dei dati al Titolare del Trattamento all'atto della conclusione o della revoca dei servizi oggetto dell'atto di affidamento, a cancellare fisicamente dai propri sistemi e dai propri archivi elettronici tutti i dati/documenti informatici di proprietà del Titolare stesso, ad esclusione dei dati legati all'attività di *Trouble Ticketing System*, i quali sono per loro natura vincolati ad autonomo criterio in materia di persistenza.

L'Ateneo si riserva di svolgere presso Cineca le ispezioni periodiche prescritte dal D.lgs. 196/2003 per assicurarsi che le proprie istruzioni vengano eseguite correttamente e che siano sempre valide e presenti le qualità di esperienza, capacità e affidabilità richieste al Responsabile del Trattamento.

#### **Elenco delle tipologie documentarie soggette a conservazione da parte di CINECA**

| <b>Tipologia documento</b>      | <b>Conservazione</b> | <b>Tempo di permanenza nell'archivio corrente</b> | <b>Versamento - periodicità</b>                                                                                                                     | <b>Formato doc.</b> |
|---------------------------------|----------------------|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <b>Registro di protocollo</b>   | Illimitata           | Illimitata                                        | Giornalmente - Versamento diretto in Conserva                                                                                                       | XML                 |
| <b>Fatture passive verso PA</b> | 10 anni              | Illimitata                                        | Settimanalmente - Versamento diretto in Conserva (in ogni caso entro i termini previsti dalla normativa in materia, 31 marzo dell'anno successivo). | XML                 |
| <b>Fatture attive verso PA</b>  | 10 anni              | Illimitata                                        | Annualmente - Versamento diretto in Conserva (in ogni caso entro i termini previsti dalla normativa in materia, 31 marzo dell'anno successivo).     | XML                 |
| <b>Registri IVA</b>             | 10 anni              | Illimitata                                        | Trimestrale - Versamento diretto in Conserva (in ogni caso entro i termini previsti dalla normativa in materia, 31 marzo dell'anno successivo).     | XML                 |

## ALLEGATO 4

### **Convenzione di Affidamento del Servizio di Conservazione, Nomina e Adempimenti del Responsabile esterno del Trattamento dei dati personali, e Affidamento all'esterno delle attività del Responsabile della conservazione, per quanto concerne UniIT**

Spettabile  
UNI IT SRL  
Via G. Galilei, 1  
38122 TRENTO (TN)

Si trascrive di seguito la:

***CONVENZIONE DI AFFIDAMENTO DEL SERVIZIO DI CONSERVAZIONE***  
*(ai sensi e per gli effetti del comma 7, dell'art. 6 del DPCM 3 dicembre 2013, recante le Regole tecniche in materia di sistemi di sistemi di conservazione)*

Parti della Convezione

- UNI IT S.R.L. (successivamente anche "CONSERVATORE" o "PARTE") con Sede Sociale in Trento, Via Galilei, 1, Capitale Sociale € 1.000.000,00.= interamente versato, Iscrizione al Registro delle Imprese di Trento, C.F. e P.IVA n. 01827210228, società appartenente al Gruppo Bancario UniCredit, in persona del Direttore Generale dott.ssa Elisabetta Pisoni,
- e
- UNIVERSITÀ PER STRANIERI DI PERUGIA (successivamente e per brevità anche "ENTE" o "PARTE"), con Sede Legale in Perugia, C.F. 80002630541 e P.IVA 01202780548, rappresentato dal Rettore Prof. Giovanni Paciullo quale Legale Rappresentante;
- Uni IT S.r.l. e Università per Stranieri di Perugia di seguito, congiuntamente: "PARTT"

**PREMESSO CHE**

- tra UniCredit S.p.A. (di seguito anche "TESORIERE") ed ENTE è stato sottoscritto un contratto di fornitura del servizio di tesoreria (di seguito anche solo "contratto");
- a seguito dell'entrata in vigore del DPCM 3 dicembre 2013, recante Regole tecniche in materia di sistemi di conservazione, l'ENTE ha rappresentato al TESORIERE l'esigenza di ottenere anche la fornitura di servizi relativi a un sistema di conservazione dei documenti informatici, ai sensi degli artt. 44 e 44-bis del Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005) del citato decreto;
- l'ENTE, consapevole del fatto che l'attività di conservazione dei documenti informatici, effettuata nel rispetto dei requisiti di legge prescritti, richiede una forte integrazione con gli applicativi di UniCredit S.p.A., ha incaricato quest'ultima di occuparsi, nel suo interesse, del coordinamento di tutte le attività necessarie per la corretta conservazione dei documenti informatici prodotti o comunque detenuti dall'ENTE;
- UniCredit S.p.A. ha individuato Uni IT Srl, già propria struttura tecnica delegata per il servizio Ordinativo Informatico a firma digitale fornito dal Tesoriere nell'ambito del contratto, quale soggetto idoneo anche a fornire i servizi di conservazione dei documenti informatici nei termini previsti dalle vigenti disposizioni di legge;

- l'Ente, ai sensi del comma 1 ter dell'art. 44 del D.Lgs 82/2005 e del comma 7, dell'art. 6 del DPCM 3 dicembre 2013, intende affidare a Uni IT Srl, in quanto conservatore accreditato ex art. 44 bis del CAD, la conservazione dei documenti in linea con quanto previsto dal Codice dell'Amministrazione digitale e delle regole tecniche innanzi richiamate;
- tra UniCredit S.p.A. e Uni IT Srl è stato sottoscritto un accordo per la fornitura di servizi di conservazione in favore dei clienti di UniCredit S.p.A.;
- ai sensi del comma 7, dell'art. 6 del DPCM 3 dicembre 2013, recante le Regole tecniche in materia di sistemi di conservazione, la conservazione può essere affidata "ad un soggetto esterno mediante contratto o convenzione di servizio che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa".

**Tutto ciò premesso, si conviene quanto segue:**

## **1. STRUTTURA E OGGETTO DELLA CONVENZIONE**

**1.1** Con la presente Convenzione le parti intendono individuare le condizioni generali e i termini in ordine ai quali il CONSERVATORE fornisce all'ENTE, anche per il tramite degli applicativi già rilasciati da UniCredit S.p.A. allo stesso, il Servizio di conservazione (di seguito anche solo "Servizio"), come meglio specificato nel manuale operativo del CONSERVATORE allegato alla presente Convenzione.

**1.2** Il Servizio, inoltre, viene erogato dal CONSERVATORE in conformità a quanto già pattuito dall'ENTE in separato contratto con il quale aveva richiesto al TESORIERE la fornitura di tale specifico servizio e che qui integralmente si richiama.

**1.3** Con la sottoscrizione della presente Convenzione, quindi, l'ENTE affida al CONSERVATORE, quale soggetto individuato dal TESORIERE, l'incarico di svolgere il processo di conservazione dei propri documenti informatici.

## **2. MODALITÀ DI FORNITURA DEL SERVIZIO**

**2.1** Per l'esecuzione del Servizio di conservazione, il CONSERVATORE mette a disposizione dell'ENTE, anche per il tramite del TESORIERE, i sistemi informatici e telematici ai quali è possibile accedere nelle modalità specificate nel Manuale operativo del CONSERVATORE, allegato alla presente Convenzione.

**2.2** Il Servizio è prestato dal CONSERVATORE solo a seguito di accettazione, effettuata anche con procedure automatizzate, dei dati e dei documenti inviati. Sono accettati esclusivamente i dati e i documenti inviati con le modalità, nei formati e nelle tempistiche concordate con l'ENTE e indicate nell'Accordo di Versamento così come stabilito all'art. 6.

**2.3** Il CONSERVATORE, ricevuto il flusso di documenti da conservare (sotto forma di uno o più pacchetti di versamento) ne controlla la conformità all'Accordo di versamento e, in caso di esito positivo, restituisce all'ENTE un rapporto di versamento contenente l'impronta del pacchetto di versamento acquisito e la data e l'ora dell'acquisizione. In caso di esito negativo del suddetto controllo, il CONSERVATORE segnala all'ENTE, mediante apposita comunicazione inviata agli indirizzi di cui al successivo art. 9, l'impossibilità di procedere correttamente alla conservazione così come previsto nel Manuale operativo allegato. È onere dell'ENTE inviare un nuovo pacchetto di versamento conforme a quanto previsto dall'Accordo di versamento.

**2.4** Il CONSERVATORE e l'ENTE possono accordarsi per la realizzazione di ulteriori controlli formali che possono portare anche alla mancata accettazione dei documenti da conservare e garantire

così quanto richiesto obbligatoriamente per la formazione dell'archivio di conservazione. I controlli e le verifiche ulteriori concordati possono essere eventualmente specificati nell'Accordo di Versamento.

2.5 Gli strumenti di controllo e verifica predisposti dal CONSERVATORE, ove utilizzati, sono completamente automatizzati e non permettono in alcun modo di conoscere il contenuto dei documenti versati in conservazione, né di verificarne eventualmente la loro correttezza sostanziale. Per tale motivo, il CONSERVATORE declina ogni responsabilità relativa al contenuto dei documenti emessi e/o conservati.

### **3. CARATTERISTICHE DEL SERVIZIO DI CONSERVAZIONE**

3.1 Il Servizio di conservazione offerto dal CONSERVATORE è sviluppato secondo quanto stabilito dal D.lgs. 82/2005 e dalle regole tecniche ivi richiamate; le firme digitali necessarie alla corretta esecuzione del Servizio sono tutte state rilasciate da Certificatori accreditati, valide e non scadute, revocate o sospese, e, ove richiesto dalla normativa, di marche temporali rilasciate sempre da Certificatori accreditati.

3.2 Le tempistiche di conservazione sono concordate con l'ENTE e vengono indicate in uno specifico Accordo di versamento di cui al successivo art. 6. Tutti i documenti da conservare dovranno essere correttamente trasmessi dall'ENTE al CONSERVATORE nei tempi, con le modalità e nelle forme indicate nell'Accordo di versamento citato.

3.3 Gli archivi di conservazione sono conservati presso i server situati in strutture gestite e controllate dal CONSERVATORE. Su richiesta da far pervenire almeno 15 giorni prima, il CONSERVATORE si impegna a permettere l'accesso degli ispettori appartenenti all'ENTE stesso o ad altre amministrazioni competenti (ad esempio sovrintendenza dei beni culturali) a propri locali e apparati hardware e software attraverso i quali è possibile accedere all'archivio di conservazione e a fornire tutte le risorse fisiche e strumentali e il supporto operativo necessari allo svolgimento delle attività ispettive.

3.4 Su richiesta dell'ENTE, da far pervenire per il tramite del TESORIERE e alle condizioni economiche meglio dettagliate nel contratto o in separato accordo tra TESORIERE e l'ENTE, il CONSERVATORE rende disponibile, anche per il tramite degli applicativi informatici già rilasciati dal TESORIERE, l'archivio di conservazione auto consistente. Tale archivio può, dietro il pagamento di un corrispettivo che sia adeguato alla quantità di dati e documenti da migrare e che sia concordato tra le parti in forma scritta, essere riversato su supporti informatici auto consultanti (CD, DVD, Memorie di massa o altri supporti di memorizzazione concordati) e consegnati all'ENTE.

3.5 Fermo restando che il ruolo di RESPONSABILE DELLA CONSERVAZIONE è individuato all'interno della struttura organizzativa dell'ENTE, il CONSERVATORE, al fine di una più agevole ed efficiente erogazione del Servizio oggetto della presente Convenzione, ha individuato, all'interno della propria struttura organizzativa, un soggetto incaricato di svolgere le attività inerenti ai compiti di RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE.

### **4. OBBLIGHI E RESPONSABILITA' DELL' ENTE**

4.1 Al fine di garantire la corretta esecuzione delle prestazioni previste dalla presente Convenzione l'ENTE si impegna a:

- dotarsi di tutti i requisiti necessari per l'accesso e la fruizione del Servizio, anche a seguito di eventuali modifiche del Servizio;
- inviare tutti i documenti che devono essere conservati digitalmente con le modalità e nei formati previsti nell'Accordo di versamento e nel rispetto delle modalità e dei termini stabiliti dalla

normativa di riferimento anche fiscale, tenuto conto dei tempi di esecuzione del ciclo di conservazione; - osservare le disposizioni stabilite nel Contratto, nella presente Convenzione e nei suoi Allegati, rispettando le modalità di fruizione del Servizio, nonché i termini di trasmissione, di spedizione, di consegna, di controllo necessari al CONSERVATORE per svolgere correttamente il Servizio.

4.2 L'ENTE, inoltre, s'impegna ad assicurare al CONSERVATORE la collaborazione necessaria affinché quest'ultimo possa dare corso alle attività previste dalla Convenzione conclusa tra le Parti, per svolgere correttamente e a regola d'arte il Servizio, mettendo altresì a disposizione dello stesso i documenti richiesti, secondo quanto previsto nella presente Convenzione e nei suoi Allegati.

4.3 A tal fine, entro 10 giorni dalla sottoscrizione della presente Convenzione e degli Allegati, l'ENTE si impegna a comunicare al CONSERVATORE il nominativo del proprio Responsabile della conservazione, quale interlocutore privilegiato del Responsabile del servizio di conservazione del CONSERVATORE.

4.4 L'ENTE si impegna a fornire al CONSERVATORE il proprio Manuale della Conservazione reso comunque conforme a quanto pattuito nel Contratto e nella presente Convenzione e, in ogni caso, prevedendo modalità di realizzazione del servizio compatibili con il Manuale operativo del CONSERVATORE allegato alla presente convenzione.

4.5 L'ENTE, più in generale, si impegna ad utilizzare il Servizio nei termini convenuti, nonché ad adoperarsi per assicurare il rispetto, da parte dei propri dipendenti e/o collaboratori, della presente Convenzione e degli Allegati; l'ENTE si impegna altresì a comunicare tempestivamente al CONSERVATORE eventuali abusi relativi al Servizio erogato da quest'ultimo, dei quali dovesse venire a conoscenza.

4.6 Qualora per la gestione e conservazione degli archivi dell'ENTE siano richiesti adempimenti e/o autorizzazioni ulteriori rispetto a quanto previsto nel Contratto, nella presente Convenzione o nel Manuale operativo del CONSERVATORE, la loro corretta richiesta o esecuzione resta a completo carico dell'ENTE.

## **5. OBBLIGHI E RESPONSABILITA' DEL CONSERVATORE**

5.1 Il CONSERVATORE si impegna a verificare il corretto funzionamento dei sistemi messi a disposizione dell'ENTE, per consentire l'utilizzo del Servizio, come previsto dalla presente Convenzione.

5.2 Al fine di assicurare la corretta erogazione del Servizio oggetto della presente Convenzione, il CONSERVATORE si impegna a:

- a) garantire l'impiego di metodologie aggiornate per la gestione degli strumenti hardware e software necessari alla realizzazione del Servizio oggetto della presente Convenzione assicurandone precisione, tempestività e sicurezza;
- b) erogare il Servizio mediante personale qualificato e dotato delle necessarie competenze, in modo continuativo e professionale nel rispetto degli standard di livello più alto del settore e dichiara che, per la fornitura degli stessi, utilizzerà le migliori conoscenze nonché metodi già sperimentati, avvalendosi, se del caso, anche dell'opera di terzi;
- c) assicurare la manutenzione dei sistemi tecnologici utilizzati nel processo di gestione e conservazione documentale, nonché il ripristino delle funzionalità degli stessi in caso di malfunzionamenti dei software utilizzati;
- d) gestire i dati e i documenti informatici dell'ENTE, oggetto del Servizio, adottando opportune misure di sicurezza informatica, logiche e fisiche, anche secondo quanto previsto dal successivo art. 7 e adottando le opportune misure organizzative e tecniche per evitare il verificarsi di divulgazioni,

comunicazioni, cessioni a terzi, riproduzioni dei dati o duplicazioni di banche dati nei casi diversi da quelli previsti dalla legge;

e) garantire la corretta custodia dei documenti conservati secondo la normativa vigente e a tal fine dichiara di aver stipulato la polizza assicurativa richiesta per i conservatori accreditati dall'Agenzia per l'Italia Digitale sui rischi industriali derivanti dalle attività di gestione, conservazione e custodia di dati e documenti elettronici;

f) effettuare un corretto trattamento dei dati personali di titolarità dell'ENTE ai sensi della normativa vigente (D.Lgs. 196/2003) e nei modi e termini previsti dall'art. 7 della presente Convenzione; g) osservare gli adempimenti di cui al D.Lgs. 81/2008 e s.m.

5.3 Salvo quanto inderogabilmente previsto dalla legge, il CONSERVATORE non risponderà di interruzione, sospensione, malfunzionamento o ritardo nell'erogazione del Servizio oggetto della presente Convenzione causati da caso fortuito o forza maggiore o da cause comunque allo stesso non imputabili come:

- errata utilizzazione o impiego atipico del Servizio da parte dell'ENTE;
- malfunzionamento del sistema informatico dell'ENTE;
- documenti trasmessi dall'ENTE contenenti dati non accurati, non corretti o non completi o non conformi a quanto previsto dall'Accordo di versamento di cui all'art. 6 della presente Convenzione;
- ogni altro evento non prevedibile e dipendente da fatti naturali o di terzi, quali catastrofi naturali, alluvioni, fulmini, incendi, etc.

5.4 Il CONSERVATORE non assume alcuna responsabilità per il mancato rispetto di tempistiche regolate dalla legge, in relazione alla tipologia documentale conservata dovuto a ritardi o inadempienze imputabili all'ENTE o ai delegati dello stesso.

## **6. ACCORDO DI VERSAMENTO**

6.1 ENTE e CONSERVATORE, al fine di garantire la corretta erogazione del Servizio, e nel rispetto di quanto previsto dallo standard ISO 14721:2012 (Open Archival Information System - OAIS) adottato dal CONSERVATORE, s'impegnano, di comune accordo, a redigere e approvare un Accordo di versamento (*submission agreement*) che regolerà tempi e modalità relativi al versamento in conservazione dei documenti dell'ENTE. Tale accordo dovrà in ogni caso prevedere tempi e modalità di versamento non in contrasto con quanto previsto dal Manuale operativo del CONSERVATORE allegato alla presente Convenzione.

## **7. RISERVATEZZA DEI DATI E DELLE INFORMAZIONI**

7.1 Tutti i dati e le informazioni concernenti le Parti, la loro organizzazione e/o la loro Direzione e/o i loro dipendenti, collaboratori, clienti e fornitori, appresi, comunicati o comunque nella loro disponibilità, saranno considerati riservati e come tali saranno trattati nel rispetto del D.Lgs. 30 giugno 2003 n. 196 (Codice privacy) e in ogni modo della vigente normativa in materia di protezione dei dati personali; tali dati resteranno comunque di proprietà e/o nella titolarità del rispettivo interessato/titolare e/o delle altre società da questi controllate o comunque ad essi collegate.

7.2 Le Parti si impegnano a garantire la riservatezza, l'integrità e la disponibilità di tali dati ed informazioni, anche alla luce delle specificità dell'attività bancaria e dell'amministrazione pubblica.

7.3 Le Parti dovranno per questo motivo proteggere detti dati ed informazioni mediante l'adozione di idonee e preventive misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme agli scopi di cui alla presente Convenzione oltre a quanto già specificamente previsto nella Convenzione stessa o nei suoi allegati in materia di misure di sicurezza fisica e logica.

7.4 Ciascuna Parte potrà trattare i dati dell'altra al solo fine e nei limiti di quanto strettamente necessario per l'esecuzione della Convenzione.

7.5 Le Parti, inoltre, garantiscono di aver adottato – anche in ragione degli adempimenti di cui, in particolare, alla presente Convenzione – le specifiche cautele previste per l'amministratore di sistema ai sensi del Provvedimento del Garante del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) e del 25 giugno 2009 (che ha parzialmente innovato, con modifiche, il provvedimento del 27 novembre 2008).

7.6 Le Parti potranno comunicare liberamente soltanto quelle informazioni che siano di pubblico dominio per atto legittimo, ovvero la cui comunicazione sia stata autorizzata per iscritto dalla Parte alla quale le informazioni si riferiscono, oppure ancora delle quali sia imposta la comunicazione in conseguenza di disposizioni di pubblica autorità o di legge o che siano legittimamente trasmesse alla Parte da soggetti terzi, i quali le abbiano a loro volta ottenute legittimamente e senza vincolo di confidenzialità.

7.7 Alla cessazione della Convenzione, ciascuna Parte dovrà restituire all'altra tutti i dati, documenti e informazioni ricevuti nell'ambito della presente Convenzione o comunque posseduti ai fini dell'esecuzione della stessa, su supporto cartaceo, magnetico o altro supporto concordato tra le Parti e/o a distruggerne tutte le copie e record dietro richiesta scritta dell'altra parte, con verbalizzazione delle relative attività di distruzione.

7.8 Gli obblighi di riservatezza dei dati e delle informazioni relativi alla presente Convenzione dovranno essere osservati anche successivamente alla cessazione, per qualsiasi motivo, della medesima Convenzione salvo diverso accordo tra le Parti.

7.9 L'ENTE garantisce che tutti gli obblighi di riservatezza in questo articolo disciplinati saranno osservati anche da ciascuno dei propri dipendenti e/o collaboratori, i quali saranno debitamente informati e tenuti, in base alle istruzioni impartite da ciascuna Parte, a trattare i dati acquisiti nell'esercizio delle mansioni/attività loro assegnate, e/o altrimenti conosciuti, con la massima cura, diligenza, riservatezza e, comunque, al solo fine di svolgere ogni attività e/o operazione necessaria per l'esecuzione della Convenzione, assicurando il rispetto degli impegni a tal fine assunti. 7.10 Qualunque violazione degli obblighi assunti potrà costituire causa di risoluzione della Convenzione, e di qualunque altro accordo o contratto esistente tra le Parti fatta comunque sempre salva la facoltà di una Parte di richiedere all'altra il risarcimento degli eventuali danni.

7.11 Ai fini di cui all'art. 29 D.Lgs. 196/2003 (Codice privacy) e ai sensi dell'art. 6, comma 8, del DPCM 3 dicembre 2013, l'ENTE conferisce al CONSERVATORE, che accetta, i compiti e le istruzioni necessarie ad eseguire le operazioni di trattamento nell'ambito della Convenzione sottoscritta, nel rispetto delle regole e dei principi di cui al D.Lgs. 196/2003 (Codice privacy) e del corretto trattamento dei dati personali. In particolare, il CONSERVATORE si impegna al rispetto delle previsioni convenzionali e assumerà, per mezzo di apposita nomina allegata alla presente Convenzione, il ruolo di responsabile esterno del trattamento dei dati, così come previsto dal Codice in materia di protezione dei dati personali.

## **8. CESSIONE DELLA CONVENZIONE**

8.1 Il CONSERVATORE si impegna a non cedere a terzi o a sub-appaltare, in tutto o in parte, la presente Convenzione senza la preventiva autorizzazione scritta dell'ENTE.

## **9. COMUNICAZIONI**

9.1 Ai fini dell'esecuzione del presente Contratto, le PARTI eleggono il proprio domicilio presso la propria sede legale e, quindi, rispettivamente

a) per quanto riguarda il CONSERVATORE:

Responsabile del servizio di conservazione: dott.ssa Elisabetta Pisoni

Indirizzo: TRENTO Via Galilei, 1 Telefono:

0461 1575697

e-mail: [uniitsegreteria@uniit.it](mailto:uniitsegreteria@uniit.it)

PEC: [uniit@legalmail.it](mailto:uniit@legalmail.it)

b) per quanto riguarda l'ENTE:

Responsabile della conservazione: dott. Giorgio Piermarini

Indirizzo: Piazza Fortebraccio 4, Perugia

Tel.: 075 5746254

PEC: [protocollo\(at\)pec.unistrapg.it](mailto:protocollo(at)pec.unistrapg.it)

9.2 Le comunicazioni spedite a mezzo raccomandata A/R avranno effetto dal momento del ricevimento, mentre quelle inviate a mezzo posta elettronica certificata avranno effetto dal momento della loro disponibilità nel server del gestore del destinatario.

9.3 Le PARTI si obbligano a comunicare, nel corso della vigenza del presente Contratto, ogni variazione dei rispettivi indirizzi. In caso di mancata comunicazione della variazione, tutte le comunicazioni che saranno effettuate in base ai vecchi recapiti avranno piena efficacia e validità.

## **10. DECORRENZA E DURATA DELLA CONVENZIONE - CESSAZIONE DEGLI EFFETTI DELLA CONVENZIONE**

10.1 La presente Convenzione obbliga entrambe le Parti al suo rispetto dal momento della sua sottoscrizione.

10.2 La Convenzione resta valida per tutta la durata del Contratto; in caso di cessazione degli effetti del Contratto (per mancato rinnovo, recesso o risoluzione anche di solo una delle parti) cessano anche gli effetti della presente Convenzione.

10.3 In caso di cessazione degli effetti della Convenzione, a qualsiasi causa imputabile, il CONSERVATORE si impegna a restituire all' ENTE tutta la documentazione e i dati di qualunque genere ricevuti da quest'ultimo per l'esecuzione del Servizio oggetto della presente Convenzione, anche per il tramite di UniCredit S.p.A., e secondo i tempi e le modalità già previste nel Contratto.

10.4 Dalla cessazione degli effetti della Convenzione è possibile solo richiedere, da parte dell'ENTE la restituzione degli archivi di conservazione e la loro successiva cancellazione.

10.5 Successivamente all'avvenuta cessazione, il CONSERVATORE si rende disponibile dietro pagamento di adeguato corrispettivo, a fornire supporto tecnico per la migrazione dei dati e dei documenti archiviati e conservati al fine di facilitarne l'ordinato trasferimento all'ENTE o ad altro soggetto da questi indicato e, in ogni caso, a rendere all'ENTE entro 6 mesi i dati relativi all'archivio di conservazione, su apposito supporto o memoria durevole.

10.6 L'ENTE riconosce e accetta di non poter avanzare alcuna richiesta di risarcimento danni nei confronti del CONSERVATORE a seguito di quanto specificato nei commi precedenti.

## **11. CLAUSOLE GENERALI**

11.1 L'eventuale nullità e/o inefficacia e/o annullamento di una delle clausole della Convenzione o degli Allegati non inficerà la validità della Convenzione e/o delle ulteriori condizioni ad essa applicabili.

11.2 L'eventuale tolleranza di una Parte all'inadempimento dell'altra ad uno o più obblighi convenzionali, non potrà in alcun modo essere considerata come rinuncia ai diritti attribuiti, per legge o per convenzione, alla Parte non inadempiente.

11.3 Salvi i casi per i quali sia previsto diversamente, le modifiche alla presente Convenzione e ai suoi Allegati saranno efficaci esclusivamente se convenute tra le Parti in forma scritta.

11.4 Il CONSERVATORE dichiara di aver preso visione del DPR 62/2013 "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del D.Lgs. 30 marzo 2001 n° 165".

11.5 Per tutto quanto non contemplato nella presente Convenzione e negli Allegati si rinvia alle disposizioni di Legge, con particolare riferimento alle norme del Codice Civile (e, in particolare, all'art. 2277 c.c. che disciplina l'appalto di servizi), del D.Lgs. n. 196/2003 (Codice privacy), della L. 633/41, del D.Lgs. 82/2005 e le regole tecniche ivi richiamate, così come successivamente integrate e modificate.

Ai sensi e per gli effetti di cui agli articoli 1341 e 1342 c.c., le Parti dichiarano, dopo attenta lettura, di aver compreso e di approvare specificamente quanto disposto dai seguenti articoli:

art. 2 (Modalità di fornitura del Servizio), art. 3 (Caratteristiche del Servizio di conservazione), art. 4 (Obblighi e responsabilità dell'ENTE), art. 5 (Obblighi e responsabilità del CONSERVATORE), art. 7 (Riservatezza dei dati e delle informazioni), art. 8 (Cessione della Convenzione), art. 10 (Decorrenza e durata della convenzione – Cessazione degli effetti della convenzione), art. 11 (Clausole generali).

Università per Stranieri di Perugia

IL RETTORE

Prof. Giovanni Paciullo

Perugia, 21 agosto 2017

#### **ALLEGATI**

- Allegato A: Nomina a Responsabile del trattamento dei dati personali
- Allegato B: Manuale operativo del Conservatore – disponibile all'indirizzo:  
[http://www.agid.gov.it/sites/default/files/documentazione/manuale\\_conservazione\\_uni\\_it\\_vers\\_1\\_4\\_con\\_testo\\_alternativo\\_nelle\\_figure.pdf](http://www.agid.gov.it/sites/default/files/documentazione/manuale_conservazione_uni_it_vers_1_4_con_testo_alternativo_nelle_figure.pdf)

## ALLEGATO 5

### **Accordi di versamento e Manuale del Conservatore, per quanto concerne CINECA, e Manuale del Conservatore per quanto concerne UniIT**

Per il Cineca, si riportano i seguenti documenti:

- ✓ *Accordo di versamento per la conservazione del registro informatico di protocollo giornaliero, del 17 maggio 2016,*
- ✓ *Accordo di versamento per la conservazione delle fatture elettroniche attive verso pubbliche amministrazioni – PA trasmesse da Titulus tramite sistema di interscambio – SDI, del 17 maggio 2016,*
- ✓ *Accordo di versamento per la conservazione delle fatture elettroniche passive e dei lotti ricevuti tramite sistema di interscambio – SDI, del 16 dicembre 2016,*
- ✓ *Accordo di versamento per la conservazione dei registri IVA, del 10 gennaio 2018,*
- ✓ *Manuale di Conservazione del Consorzio Interuniversitario CINECA.*

Per UniIT, si riportano i seguenti documenti:

- ✓ *Manuale di Conservazione di UniIT.*

*Per l'Accordo di versamento per la conservazione dei documenti contabili, si rimanda alla Convenzione di Affidamento del Servizio di Conservazione, già riportato in Allegato 4*