ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
AREA SISTEMI E SERVIZI INFORMATICI

SERVIZIO DI FIRMA DIGITALE REMOTA E TIMBRO DIGITALE PER LE ESIGENZE DELL'ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA

CONDIZIONI PARTICOLARI DI CONTRATTO

Il RUP
Ing. Enrico Lodolo

1. Premessa

Il presente documento integra le condizioni previste dai bandi MEPA le quali prevalgono in caso di contrasto con le disposizioni del bando stesso. Il presente documento precisa altresì l'oggetto, le modalità di erogazione del servizio richiesto e la qualità attesa.
L'Ateneo, attraverso l'Area dei Sistemi e Servizi Informatici (d'ora in poi CESIA), intende realizzare il servizio in oggetto.

2. Oggetto della fornitura

Il servizio richiesto ha per oggetto l'affidamento del servizio a consumo di Firma Digitale Remota, Timbro Elettronico e servizi accessori.
Tutti i servizi specificati nel presente capitolo devono essere tassativamente forniti nel rispetto delle normative vigenti e delle relative evoluzioni (quali ad esempio Codice 9 Amministrazione Digitale (CAD), Regolamento eiDAS, ecc.) per tutta la durata contrattuale.
La Firma Digitale rappresenta un processo informatico che consente la dimostrazione di autenticità di un messaggio o di un documento digitale. La firma digitale apposta su un documento elettronico ne garantisce validità, integrità, autenticità e la non ripudiabilità.
Il Timbro Digitale, detto anche contrassegno, è la tecnologia che consente di creare documenti informatici (ad esempio certificati anagrafici rilasciati dai Comuni, certificati rilasciati dalle Università, ecc.) validi legalmente anche dopo la stampa in analogico.
I servizi richiesti devono essere forniti dall'Impresa attraverso una infrastruttura cloud, compatibile con architetture virtualizzate, che assicuri la continuità operativa; eventualmente potrà prevedere una componente infrastrutturale software installata localmente su sistemi operativi open.
I servizi richiesti devono essere erogati adottando le migliori pratiche e tecnologie disponibili relativamente a tutti gli aspetti di conservazione delle credenziali, dei codici segreti, dei flussi di comunicazione e delle procedure di ripristino dei dati in caso di malfunzionamenti e/o incidenti.
Le interfacce web e mobile devono essere integrabili a sistemi di autenticazione esterni attraverso interfacce standard SAML2.0 e OpenID Connect. I servizi devono essere forniti nel pieno rispetto delle normative vigenti, comprese quelle sul trattamento dei dati personali, prevedendo anche un adeguamento costante e continuo delle funzionalità nel rispetto delle relative evoluzioni.
Si sottolinea che tutti i documenti che devono essere sottoposti al processo di Firma Digitale e/o Timbratura elettronica devono rimanere all'interno del dominio dell'Ateneo senza essere inviati ai sistemi dell'Impresa. Le informazioni inviate ai sistemi dell'Impresa devono includere un set minimale di informazioni tale da garantire una gestione corretta e limitata degli aspetti di privacy.
Tutte le attività dovranno essere svolte secondo le procedure e le modalità stabilite da CESIA che potrà, in qualsiasi momento, verificarne lo svolgimento da parte dell'Impresa, richiedere chiarimenti ed approfondire le modalità di erogazione dei servizi anche al fine di migliorare i processi e le procedure. A tale scopo saranno organizzati incontri periodici con l'Impresa per discutere sia l'andamento generale del servizio sia specifiche problematiche tecniche riscontrate.
L'Impresa dovrà svolgere, sotto la propria responsabilità, tutte le attività nel pieno rispetto delle normative vigenti con particolare riferimento agli aspetti di sicurezza.

2.1 Servizio di Firma Digitale

Il servizio di Firma Digitale deve garantire il processo di firma da parte del personale dell'Ateneo e la disponibilità di interfacce per permettere l'integrazione di una, o più applicazioni, del dominio dell'Ateneo (ad esempio applicazioni di verbali di commissioni, ecc.).

Il servizio di Firma Digitale deve prevedere, nel rispetto delle normative, regolamenti e regole tecniche vigenti, le seguenti tipologie di firme:

- Firma Digitale Remota;
- Firma Digitale Automatica;
- Firma Digitale "One Shot" o Temporanea.

Per servizio di Firma Digitale remota si intende una "particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM (Hardware Security Module), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse". Il dispositivo sicuro di firma HSM su cui sono installati i certificati qualificati e le chiavi private dei diversi firmatari sono gestiti in remoto e il controllo esclusivo delle chiavi private da parte dei titolari stessi avviene tramite l'utilizzo di codici OTP (One Time Password), create da apposite modalità gestite dall'utente.
Per servizio di Firma Digitale automatica si intende una "particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo". La firma digitale automatica consente comunque di eseguire firme massive su più documenti con un'unica richiesta di PIN in fase di attivazione e senza che vi sia la necessità da parte del firmatario di presidiare il dispositivo sicuro per la generazione della firma digitale.
Per servizio di Firma Digitale "One Shot" o Temporanea si intende un servizio con caratteristiche simili a quello del servizio di Firma Digitale remota, che consente di eseguire firme su uno o più documenti per un periodo di tempo limitato tramite l'emissione di un certificato di firma di validità limitata a poche ore o pochi giorni.
Il servizio di Firma Digitale richiesto deve gestire l'accesso ai servizi di marcatura temporale di "Time Stamp Authorities" attraverso i protocolli e formati previsti dalla normativa vigente. La Marca Temporale è il risultato di una procedura informatica – detta servizio di marcatura temporale – grazie alla quale si attribuisce a un documento informatico un riferimento temporale opponibile a terzi.
Il servizio di Firma Digitale deve prevedere le seguenti caratteristiche minime:

- disponibilità di una interfaccia web utilizzabile da parte degli utenti RAO (Registration Authority Officer) e dagli utenti finali, fruibile da ogni versione di piattaforme Linux, Windows, Mac;
- disponibilità di API (REST/SOAP) e il supporto per l'integrazione di applicazioni dell'Ateneo, sia per quanto concerne i processi utenti (ad esempio, iscrizione dell'utente, gestione del certificato remoto, ecc) che i processi RAO;
- utilizzo di una firma qualificata emessa da Certificatore Accreditato presso AgID;
- gestione delle funzioni di firma previste dalla normativa (firma singola, firma multipla parallela, controfirma);
- disponibilità di servizi di verifica della firma di un documento e della validità del certificato sia via web che attraverso API;
- disponibilità di applicazioni desktop e web, utilizzabili anche attraverso dispositivi mobili, per l'apposizione della firma ad un documento, fruibile da ogni versione di piattaforme Linux, Windows, Mac;
- utilizzo di soluzioni che integrano certificatori di firma digitale accreditati secondo le normative;
- produzione di file firmati digitalmente con i seguenti formati:

  - CAdES, secondo le specifiche ETSI TS 101 733 CAdES;
  - PAdES, secondo le specifiche ETSI TS 102 778;
  - XAdES, secondo le specifiche ETSI TS 101 903 XAdES;
- utilizzo dei seguenti algoritmi di firma:
  - RSA (512, 1024, 2048, 4096 bit);
  - crittografia ellittica ECDSA (Elliptic Curve Digital Signature Algorithm);
- presenza di un meccanismo per sbloccare la firma del documento che deve avvenire tramite l'utilizzo di codici OTP (One Time Password), create da appositi dispositivi gestiti dall'utente: ad esempio via SMS, email e mobile app. Si precisa che il servizio non deve includere il meccanismo di trasmissione di SMS, ma solo l'integrazione con un gateway SMS che il CESIA deve poter scegliere senza vincoli;
- il meccanismo per lo sblocco della firma del documento deve prevedere nel caso di mobile app un meccanismo out of band per il secondo fattore ovvero la possibilità di trasmettere il secondo fattore direttamente dalla app al servizio di verifica senza richiede un inserimento manuale della OTP da parte dell'utente finale;
- fornitura di una applicazione mobile nativa per il servizio di firma che supporti le principali piattaforme: Android, IOS ed eventuale SDK per la customizzazione e personalizzazione; l'applicazione mobile deve essere corredata da dichiarazione sull'accessibilità che evidenzi il rispetto della normativa vigente;
- completa integrazione con il Servizio di Timbro Digitale richiesto nel presente documento.

2.2 Servizio di Timbro Digitale

Il servizio di Timbro Digitale deve essere accessibile da una o più applicazioni del dominio dell'Ateneo consentendo di apporre sui documenti firmati digitalmente un contrassegno elettronico a norma di legge.

Il servizio di Timbro Digitale deve avere come output un file PDF con applicato un glifo di dimensioni contenute, indipendentemente dalle dimensioni del documento originale. Inoltre, il servizio deve permettere la personalizzazione del contenuto del timbro digitale, attraverso l'inserimento di specifici metadata e dati descrittivi del documento.

Il servizio di Timbro Digitale deve prevedere le seguenti caratteristiche minime:

- essere conforme alla normativa vigente e, in particolare, al CAD e alle linee guida pubblicate da AgID;
- consentire una integrazione con applicazioni attraverso API;
- permettere la timbratura di documenti informatici con meccanismi che non richiedano la trasmissione dei documenti fuori dal dominio dell'Ateneo. I documenti oggetti di timbratura devono poter essere in formato PDF e in altri formati;
- fornire meccanismi di verifica di validità del documento timbrato attraverso applicazioni web e/o mobili, ovvero attraverso app native scaricabili gratuitamente dagli store Google Play, Microsoft e Apple e utilizzabili gratuitamente;
- fornire la possibilità di inserire nel timbro digitale ulteriori informazioni accessibili anche da un utente non provvisto di sistema di verifica (ad esempio URL di accesso al documento originale, codice di accesso, ecc.).

2.3 Servizi accessori e dimensionamento

Una indicazione di massima dei volumi presunti di parte degli elementi costituenti il servizio sono:

- 10.000 certificati di firma digitale attivi
- 200.000 timbrature digitali all'anno

- 40.000 marcature temporali all'anno
- 5.000 riconoscimenti tramite SPID all'anno

Di seguito un elenco non esaustivo dei servizi che si andranno ad acquisire per cui si richiede una quotazione economica, con la specifica che, essendo il servizio di firma in costante evoluzione, sarà possibile nel corso del presente contratto acquisire ulteriori servizi forniti dall'Impresa:

- Certificato di firma qualificata: valore annuo unitario omnicomprensivo per utente;
- Certificato di firma automatica: valore annuo unitario omnicomprensivo per utente;
- Marcatura Temporale: valore unitario omnicomprensivo;
- Timbro elettronico: valore unitario omnicomprensivo;
- Sigillo qualificato: valore unitario omnicomprensivo;
- Riconoscimento tramite RAO dell'Impresa: valore unitario omnicomprensivo;
- Riconoscimento tramite RAO di Ateneo: valore unitario omnicomprensivo;
- Riconoscimento tramite SPID: valore unitario omnicomprensivo;
- Firma "One shot": valore unitario omnicomprensivo;
- Corso RAO a consumo: valore unitario omnicomprensivo;
- Sviluppo e personalizzazione a consumo: valore orario omnicomprensivo.

Sono da ritenersi parte integrante della fornitura le seguenti prestazioni:

- Conservazione e gestione dei moduli di richiesta dei certificati;
- Applicazione mobile con funzione di Token per OTP;
- Applicazione desktop per la firma e funzioni correlate alla firma e verifica di documenti;
- Integrazione con SSO di Ateneo.

3. Procedure operative

L'Impresa dovrà garantire tutti i servizi minimi richiesti secondo le modalità riportate di seguito. I servizi richiesti avvengono con modalità "a consumo", sia in modalità continuativa che a seguito di richieste da parte del CESIA.

L'Impresa deve garantire i servizi richiesti nel presente documento indipendentemente dalle giornate-uomo necessarie ad ottenere il risultato. La relativa offerta economica sarà quindi da esplicitare a corpo e onnicomprensiva. Non è riconosciuto all'Impresa nessun tipo di rimborso aggiuntivo, quali - a mero titolo esemplificativo e non esaustivo - quelli per spese di trasferta.

I servizi richiesti dovranno essere erogati da remoto e l'Impresa dovrà indicare un referente che sarà il punto di contatto per il CESIA per tutte le attività oggetto del presente appalto. L'Impresa dovrà svolgere tutte le attività richieste utilizzando propri mezzi e dovrà rigorosamente documentare periodicamente e durante tutta la durata contrattuale tutte le attività pianificate e svolte.

L'Impresa potrà organizzare il proprio lavoro relativo all'oggetto di questo appalto nel modo che ritiene più idoneo per dare la migliore copertura dei servizi richiesti, fermo restando che darà assoluta trasparenza al CESIA delle procedure messe in atto, della organizzazione e della logistica relativa. Il tutto nel rispetto dei livelli di servizio richiesti.

L'Impresa dovrà erogare i servizi oggetto di fornitura principalmente da una propria sede operativa e mettendo a disposizione personale qualificato per lo svolgimento delle attività richieste, garantendo un'adeguata professionalità e competenza dello stesso.

L'Impresa dovrà mettere a disposizione del CESIA dei punti di contatto raggiungibili con le più ampie modalità telematiche per tutto l'arco della giornata e per tutti i giorni dell'anno (H24 x 7 x 365) dai locali dell'Impresa secondo procedure stabilite dal CESIA per ricevere le segnalazioni e le richieste. Gli aspetti operativi relativi allo svolgimento dei servizi saranno concordati tra il CESIA e l'Impresa.

L'Impresa dovrà inoltre mettere a disposizione una lista di contatti per le procedure di escalation, che saranno i punti di contatto per il CESIA per tutte le attività ed i servizi richiesti.
All'avvio di ciascun servizio, il CESIA provvederà a fornire all'Impresa una descrizione esaustiva delle esigenze, delle applicazioni e delle piattaforme per i servizi richiesti nonché tutte le informazioni e i riferimenti necessari per lo svolgimento delle attività.
Il CESIA metterà a disposizione dell'Impresa i sistemi e gli applicativi, accessibili da remoto, necessari per lo svolgimento delle attività oltre ai sistemi di trouble ticketing. Tutte le attività dovranno essere tracciate e aggiornate tempestivamente nei sistemi di trouble ticketing decisi dal CESIA.
La modalità di fornitura dei servizi richiesti deve prevedere, di norma, un incontro settimanale anche per via telematica per verificare lo stato di avanzamento lavori e la pianificazione delle attività.
Nella fase di avvio di ciascun servizio, la formulazione della richiesta di servizio all'Impresa da parte del CESIA potrà avvenire per e-mail o tramite incontro convocato presso la sede del CESIA o da remoto. In tale richiesta verranno specificate le esigenze specifiche ed una stima del tempo di esecuzione.
L'Impresa dovrà presentare un piano dettagliato delle attività precisando i tempi di lavoro effettivi necessari per ciascuna fase e dovrà fornire motivazioni degli eventuali scostamenti rispetto alla stima elaborata.
Durante la fase realizzativa, nel rispetto del piano temporale condiviso e approvato l'Impresa dovrà mantenere un costante confronto e aggiornamento con i referenti del CESIA sullo stato di avanzamento dei lavori e sulle scelte effettuate oltre a fornire un resoconto dettagliato sull'attività svolta, ivi comprese eventuali criticità riscontrate sia tecniche che temporali.
Eventuali modifiche alle attività, e alla relativa tempistica, o azioni risolutive delle criticità riscontrate dovranno essere proposte dall'Impresa ed approvate dal CESIA.
Le attività nella fase di avvio devono includere tutto quanto è necessario per la messa in produzione dei servizi richiesti. A titolo puramente indicativo e non esaustivo, le attività includono:

- supporto all'avvio del singolo servizio;
- supporto all'installazione della componente infrastrutturale software negli ambienti degli Enti, ove è applicabile;
- disponibilità di ambiente di test con possibilità di integrazione di sistemi di prova e supporto al relativo utilizzo;
- svolgimento di tutti i test e le verifiche di funzionamento per la messa in produzione dei servizi.

A completamento delle attività, il CESIA procederà alla validazione del risultato, della relativa documentazione concordata. Eventuali giornate necessarie ad apportare correzioni necessarie per la validazione del risultato o della documentazione, successiva al termine di consegna stabilito, saranno considerate a tutti gli effetti uno slittamento del tempo di esecuzione delle attività. La validazione del risultato da parte del CESIA dà il via alla decorrenza dei canoni relativi ai servizi.
Le attività nella fase di erogazione devono includere tutto quanto è necessario per il corretto funzionamento dei servizi richiesti nel rispetto delle normative e relative evoluzioni. A titolo puramente indicativo e non esaustivo, le attività includono:

- verifica costante del funzionamento dei servizi in tutte le loro componenti attraverso adeguate modalità e strumenti di supervisione e monitoraggio che includono le eventuali componenti infrastrutturali locali;

- rilevazione di eventuali allarmi e problematiche, analisi degli stessi, conduzione di attività di troubleshooting, determinando la natura e l'impatto del problema e attivando le azioni necessarie per la relativa risoluzione nel rispetto degli SLA;
- monitoraggio, diagnosi e risoluzione dei malfunzionamenti degli applicativi, dei server e dei sistemi ivi compresi le integrazioni con le applicazioni e le piattaforme;
- monitoraggio degli allarmi, diagnosi di possibili guasti e coordinamento con il CESIA;
- ricezione di segnalazioni dal CESIA o dai soggetti terzi autorizzati coinvolti nella gestione dei sistemi e dei servizi, analisi delle stesse e attivazione delle azioni previste secondo le procedure stabilite dal CESIA;
- inserimento e successivo aggiornamento di tutte le richieste e segnalazioni nel sistema di trouble ticketing secondo modalità operative che saranno comunicate all'Impresa dal CESIA;
- verifica della qualità del servizio offerto attraverso opportuna reportistica e incontri programmati o conferenze audio e/o video;
- oltre al servizio attivo ed operativo per tutto l'arco della giornata e per tutti i giorni dell'anno, l'Impresa dovrà mettere a disposizione una lista di contatti per le procedure di escalation, che saranno i punti di contatto del CESIA o dei soggetti terzi autorizzati per tutte le attività ed i servizi richiesti.

L'Impresa dovrà svolgere le attività con la massima puntualità e attenzione e sarà responsabile di eventuali danni, di qualunque specie, che dovesse procurare ai beni o alle persone dell'Ateneo derivanti dall'espletamento dei servizi oggetto di fornitura.
Durante lo svolgimento dei servizi, l'Impresa è tenuta a fornire al CESIA una rendicontazione periodica, ovvero reportistica bimestrale, inerente alla tendenza dei servizi erogati, secondo le indicazioni del CESIA.

4. Disponibilità del servizio, qualità e penali

In merito alla tempistica per le attività oggetto del presente avviso e della successiva richiesta di offerta si applicheranno le penali descritte in seguito, fermo restando quanto previsto al paragrafo "Penali" del presente documento.
Per ciascun servizio, si applicherà una penale di € 100,00 per ogni giorno solare di ritardo rispetto alla tempistica approvata per l'avvio in produzione, anche per le singole fasi definite nel piano di dettaglio.
Il periodo di osservazione per la misurazione dei livelli dei servizi richiesti e per il calcolo delle penali ad essi associate è stabilito in 2 mesi solari con una finestra temporale di erogazione di tutto l'arco della giornata e per tutti i giorni dell'anno (H24 x 7 x 365).
Si definisce:

- Disponibilità:
  - Disponibilità del singolo servizio: è definita come la percentuale di tempo durante il quale il servizio è operativo e svolge tutte le funzioni previste, rispetto alla finestra temporale di erogazione e al periodo di osservazione.
- Tempi:
  - Tempo di presa in carico: tempo massimo intercorrente tra la ricezione della richiesta o segnalazione e la conferma di presa in carico con l'indicazione del numero di ticket.
  - Tempo di risoluzione: tempo massimo intercorrente tra la ricezione della richiesta o segnalazione o comparsa del malfunzionamento e la risoluzione del problema.

I servizi dovranno essere erogati rispetto ai seguenti livelli di servizio (SLA):

- Disponibilità di ciascun servizio: 99.97% pari a 26 minuti di indisponibilità su due mesi;

- Tempo presa in carico: 60 minuti (30 minuti in caso di indisponibilità di tutti i servizi)
- Tempo di risoluzione: 120 minuti (60 minuti in caso di indisponibilità di tutti i servizi)

Qualora non ottemperi ai livelli di servizio sopra riportati, l'Impresa sarà soggetto alle seguenti penalità:

- disponibilità del Servizio: 100 € per ogni riduzione dello 0.01%, o sua frazione;
- tempo presa in carico: 100 € per ora, o sua frazione, di scostamento;
- per ogni giorno di ritardo nella consegna della reportistica periodica: 50 €.

Per il calcolo delle penali si considera come scostamento dagli SLA, nel periodo di osservazione, la sommatoria dei minuti eccedenti quelli consentiti, per ogni parametro identificato e per ogni servizio.

Nella reportistica, l'Impresa, oltre ad indicare i valori previsti negli SLA ed effettivamente misurati, dovrà indicare per ciascuno di essi il calcolo analitico delle penali eventualmente dovute. Il CESIA si riserva comunque la facoltà di verificare la correttezza del calcolo analitico delle penali indicato nella suddetta reportistica, sia mediante strumenti propri sia richiedendo all'Impresa puntuale verifica sui propri e dati alla base del calcolo delle penali.

5. Durata del contratto

Il contratto decorre dal 26/09/2022 fino al 31/03/2024 o potrà avere una minore durata determinata dal raggiungimento anticipato dell'importo massimo complessivo.

Il contratto potrà essere eventualmente prorogato ai sensi dell'Art. 106 c. 11 del D.Lgs. 50/2016 tramite invio di una PEC per un periodo massimo di 12 mesi e comunque non oltre il raggiungimento dell'importo massimo complessivo.

6. Valore del contratto

Il valore economico del contratto sarà pari a € 138.000 iva esclusa.

7. Responsabilità dell'Impresa

L'Impresa è responsabile, anche a nome dei propri dipendenti, dei danni diretti ed indiretti al CESIA o a terzi, di qualsiasi genere, derivanti dallo svolgimento o dal mancato svolgimento del servizio oggetto dei contratti, dell'uso o dal mancato uso dei prodotti, per violazioni di brevetti e diritti d'autore ed imitazione servile dei prodotti altrui, danni diretti all'Università e/o a terzi originati da vizi e difetti dei prodotti (DPR 224/88), mancanza delle caratteristiche qualitative pattuite, ritardata consegna, difetti di funzionamento per cattiva manutenzione, ad eccezione di quelli dovuti a cause di forza maggiore, fatto del terzo, responsabilità del CESIA e/o dei suoi dipendenti e collaboratori.

Le cause di forza maggiore indipendenti dalla volontà dell'Impresa che possono influire sulla regolarità della prestazione andranno tempestivamente segnalate e idoneamente documentate.

8. Trattamento dati personali

Per l'esecuzione del presente appalto, in qualità di titolare del trattamento, l'Ateneo nominerà una persona individuata dall'Impresa come Responsabile dei dati personali trattati in esecuzione dei compiti e delle funzioni stabiliti dall'appalto stesso, come da allegato (All.1).

Le parti, in relazione all'affidamento del presente appalto, in relazione al trattamento di dati personali effettuati in esecuzione dello stesso, si danno reciprocamente atto di aver preso visione e compreso, ai sensi dell'art. 13 del Regolamento (UE) 2016/679 (Regolamento generale sulla protezione di dati personali), tutte le informazioni riferite agli operatori economici e fornitori di beni e servizi. L'informativa inerente al trattamento di dati dell'Impresa da parte dell'Alma Mater Studiorum – Università di Bologna è pubblicata alla pagina https://www.unibo.it/privacy.

9. Report servizi erogati

L'Impresa dovrà rilasciare uno storico riepilogativo dei servizi erogati relativo ad ogni singolo bimestre.
L'Impresa dovrà altresì fornire uno storico riepilogativo dei servizi erogati relativo ad ogni anno.

10.Fatturazione e pagamenti

L'Impresa si obbliga a rispettare gli obblighi di fatturazione elettronica con le modalità previste dalla normativa vigente (DM 55/2013).
L'emissione della fattura dovrà avvenire con cadenza bimestrale posticipata di importo uguale all'effettivo costo dei servizi erogati.
La fattura dovrà essere intestata a: Area Sistemi e Servizi Informatici – CESIA Alma Mater Studiorum Università di Bologna – Viale Filopanti nr. 3 – 40126 Bologna – C.F.80007010376 - PIVA 01131710376.
La fattura dovrà obbligatoriamente riportare:

- il numero del contratto MEPA;
- il codice CIG;
- la seguente indicazione "scissione di pagamento" ai sensi dell'art. 2 co 1 del DM 23/1/2015;
- codice IPA OAHLWA.

Il pagamento avverrà entro 30 gg dalla data di arrivo della fattura, previo esito positivo delle verifiche di legge (DURC ed EQUITALIA) e previo rilascio del visto di regolare esecuzione del servizio da parte di uno dei referenti del CESIA.

11.Risoluzione del contratto

Il CESIA avrà diritto di risolvere il contratto ai sensi dell'art. 1456 cod. civ. (clausola risolutiva espressa) nei seguenti casi:

- frode nella esecuzione del servizio;
- uso improprio dei sistemi e dei contenuti informativi;
- inadempienza accertata alle norme di legge sulla prevenzione degli infortuni, la sicurezza sul lavoro e le assicurazioni obbligatorie delle maestranze, nonché in caso di mancato rispetto dei contratti collettivi di lavoro;
- sospensione o riduzione del servizio da parte dell'Impresa senza giustificato motivo;
- ricorso al subappalto in modalità difformi da quanto previsto dalle norme vigenti.

Ove si verifichino deficienze e inadempienze tali da incidere sulla regolarità e continuità del servizio, il CESIA potrà provvedere d'Ufficio ad assicurare direttamente, con oneri a carico dell'Impresa, il regolare funzionamento del servizio stesso.
Qualora si addivenga alla risoluzione del contratto, per le motivazioni sopra riportate, l'Impresa sarà tenuta al rigoroso risarcimento di tutti i danni, diretti ed indiretti, ed alla corresponsione delle maggiori spese che il CESIA dovrà sostenere per il rimanente periodo contrattuale.

12.Imposta di bollo

L'imposta di bollo è a carico dell'Impresa; il versamento all'Erario è a carico dell'Ateneo in modalità virtuale come da autorizzazione nr. 140328 del 13/12/18. L'importo di nr. 1 marca da bollo corrisponde a € 16,00.
A seguito della valutazione dell'offerta e al generarsi del documento di stipula, verrà comunicato l'importo da pagare. L'Impresa provvederà al versamento della somma corrispondente sul conto corrente del CESIA presso: Istituto Cassiere Credit Agricole Italia S.p.A., Via Guglielmo Marconi, 16 – 40126 Bologna; IBAN IT 28 X0623 00240 2000057848910 conto intestato al CESIA – causale versamento bollo "CESIA TD n. …..".

Non appena effettuato il versamento, l'affidatario si impegna ad inviare al CESIA la contabile del bonifico. Solo al ricevimento della stessa, il CESIA procederà alla stipula firmata digitalmente del contratto generato dal sistema MEPA.

13.Foro competente

Per tutte le controversie comunque attinenti all'interpretazione o all'esecuzione del contratto, è stabilita la competenza esclusiva del Foro di Bologna.

Atto di designazione quale responsabile del trattamento

ex art. 28 del Regolamento (UE) 2016/679

Il titolare del trattamento dei dati personali, *l'Alma Mater Studiorum Università di Bologna*, con sede legale in *via Zamboni 33, Bologna (BO)*, P. IVA: *01131710376*, in persona *del Magnifico Rettore*, quale rappresentante legale (di seguito indicato come "titolare")

e

[inserire dati identificativi del responsabile del trattamento], con sede legale in *[indicare sede legale], [codice fiscale]* in persona di *[indicare il legale rappresentante]*, quale rappresentante legale (di seguito indicato come "responsabile")

(entrambe di seguito collettivamente indicate come le "parti")

CONSIDERATO

- il Regolamento (UE) 2016/679 del 27 aprile 2016 (Regolamento generale sulla protezione dei dati personali, di seguito, per brevità, "Regolamento") e la vigente normativa nazionale in materia di protezione dei dati personali;
- l'*Accordo* _____ sottoscritto tra *l'Alma Mater Studiorum Università di Bologna, con sede in via Zamboni 33, Bologna (BO), P. IVA: 01131710376* e _____, con sede in via _____, _____ (__), P. IVA _____;
- la necessità e l'opportunità di individuare la figura del responsabile del trattamento *ex* art. 28 del Regolamento.

convengono e stipulano quanto segue:

1. Oggetto

Il titolare designa *[indicare nominativo del responsabile]* quale responsabile, *ex* art. 28 del Regolamento, nei limiti e alle condizioni indicate al presente atto.
In particolare, il responsabile potrà effettuare il trattamento per le finalità indicate dall'art. _____ dell'*Accordo/Contratto* sopra citato, secondo modalità connesse a tale scopo.
Il trattamento dei dati dovrà limitarsi alle operazioni strettamente necessarie per _____.
Rimane inteso che, per quanto non direttamente disciplinato in questa sede, trovano applicazione le disposizioni di cui al contratto sopra richiamato stipulato tra le parti.

2. Descrizione del trattamento

Il responsabile è designato e autorizzato a elaborare, per conto del titolare, i dati personali necessari per eseguire i trattamenti descritti nel presente atto di designazione.
Il titolare definisce i seguenti elementi identificativi del trattamento dei dati affidati al responsabile:

Data del Contratto	
Durata del trattamento	*(indicare la durata del rapporto previsto);*
Finalità del trattamento e natura del trattamento	*(riportare con precisione i compiti e le funzioni assegnate al Responsabile. In particolare,*

	occorre indicare il tipo di operazioni che dovrà eseguire nell'ambito del trattamento (per esempio, riprese, registrazione, archiviazione di immagini) e le finalità del trattamento (ad esempio, rilevamento d'ingresso illegale). Questa descrizione dovrebbe essere il più completa possibile a seconda della specifica attività di trattamento in modo da permettere a soggetti esterni (ad esempio, autorità di controllo) di capire il contenuto e i rischi del trattamento affidato al Responsabile)
Tipo di dati personali	*(riportare la tipologia di dati personali che saranno oggetto del trattamento dati. Per esempio: immagini video di persone in entrata e uscita dalla struttura. In caso di categorie particolare di dati, occorre almeno specificare quali tipi di dati sono interessati, ad esempio "informazioni riguardanti cartelle cliniche" o "informazioni sul fatto che l'interessato sia membro di un sindacato");*
Categorie di interessati	*A titolo esemplificativo:* ☐ *Dipendenti* ☐ *Docenti* ☐ *Assegnisti* ☐ *Dottorandi* ☐ *Studenti* ☐ *Aspiranti collaboratori* ☐ *Studenti 150 ore* ☐ *Fornitori* ☐ *Clienti* ☐ *Collaboratori esterni* ☐ *Minori* ☐ *Altri soggetti da identificare nel caso di specie*

3. Responsabile del trattamento dei dati personali con mansioni di amministratore di sistema

Al responsabile sono altresì affidate mansioni da amministratore di sistema, in quanto soggetto che per esperienza, capacità e affidabilità fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il responsabile, pur non essendo preposto a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), è nominato a svolgere specifiche fasi lavorative che, se non svolte nel rispetto della legge e dei regolamenti d'Ateneo, potrebbero comportare delle criticità rispetto alla protezione dei dati.

In particolare, il responsabile, oltre alle misure di sicurezza indicate dall'art. 12, si impegna a predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) dell'amministratore ai sistemi di elaborazione e agli archivi elettronici (nella sua qualità di "amministratore di sistema"). Tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Il responsabile si impegna a verificare l'operato delle persone autorizzate con funzioni di amministratore di sistema, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. A tal fine, il titolare potrà, in qualsiasi momento, chiedere eventuale documentazione che attesti le avvenute verifiche periodiche.

Il responsabile dovrà rendere conoscibili in qualsiasi momento gli estremi identificativi delle persone fisiche amministratori di sistema, con l´elenco delle funzioni ad essi attribuite. Tale documento dovrà essere aggiornato e reso disponibile in caso di accertamenti anche da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, il responsabile si impegna a rendere edotte tutte le persone da lui autorizzate con funzioni di amministratore di sistema che i loro nominativi potrebbero essere comunicati all'interno dell'organizzazione del Titolare.

Commentato [A1]: Da inserire solo nel caso in cui il compito/funzione del Responsabile riguardi anche funzioni di amministratore di sistema.

4. Obbligazioni del responsabile

Il responsabile si impegna, a titolo esemplificativo, a:

1. trattare i dati personali necessari per la fornitura e la prestazione dei servizi specificati nell'*accordo/contratto*, come sopra individuato e, successivamente agendo esclusivamente sulla base delle istruzioni documentate e fornite dal titolare, anche successivamente;
2. informare immediatamente il titolare qualora ritenga che un'istruzione costituisca una violazione della vigente normativa nazionale ed europea in materia di protezione dei dati personali;
3. informare immediatamente il titolare qualora sia tenuto, per via della propria organizzazione, a trasferire i dati verso un paese terzo o verso un'organizzazione internazionale, ai sensi del diritto dell'Unione o del diritto dello Stato membro a cui è soggetto, prima di avviare il trattamento;
4. garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto;
5. garantire, con riferimento ai propri strumenti, prodotti, applicazioni o servizi, il rispetto dei principi di "*Privacy by design*" e "*Privacy by default*" così come stabilito all'art. 25 del Regolamento;
6. assicurare che il proprio responsabile della protezione dei dati personali collabori e si tenga, se necessario, in costante contatto con il responsabile della protezione dei dati del titolare;
7. operare in modo tale che i dati personali trattati in esecuzione del presente atto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal responsabile, o da un sub-responsabile;
8. assistere il titolare nelle riunioni relative all'obbligo dell'adozione di misure tecnico-organizzative adeguate a garantire la sicurezza dei dati personali trattati;
9. adottare le misure di sicurezza dichiarate e definite dalla legge applicabile, verificandone periodicamente l'appropriatezza e adottando ogni altra misura che il responsabile ritenga opportuna per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, anche per ciò che concerne la trasmissione di dati su una rete;
10. procedere, se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento, su richiesta del Titolare, al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa che sia stata eventualmente omessa);
11. conservare i dati personali garantendo la separazione di tipo logico dai dati personali trattati per conto di terze parti o per proprio conto.

5. Persone autorizzate al trattamento

Salvo i casi previsti dalla normativa vigente, il responsabile non può comunicare a terzi o trasmettere a soggetti non autorizzati i dati personali di cui venga a conoscenza, né utilizzarli autonomamente per scopi diversi da quelli sopra menzionati.
Il responsabile garantisce l'affidabilità dei soggetti afferenti la propria struttura o comunque sottoposti al suo controllo, i quali devono utilizzare i dati per l'esecuzione delle prestazioni derivanti dai rapporti e dalle attività sopra indicate.
Il responsabile assicura, inoltre, che gli stessi abbiano ricevuto adeguata formazione con riferimento alla protezione e gestione dei dati personali. Il responsabile garantisce altresì che siano vincolati al rispetto di obblighi di riservatezza non meno onerosi di quelli previsti nel presente documento relativamente al trattamento dei dati personali e alle misure di sicurezza utilizzate.
In ogni caso il responsabile sarà direttamente ritenuto responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.
Il responsabile assicura che l'accesso ai dati sia rigorosamente limitato ai soggetti che, in ragione del ruolo e del compito svolto, abbiano effettiva necessità di accedere ai dati.

6. Eventuale trattamento dei dati personali fuori dallo Spazio Economico Europeo

Laddove il responsabile debba effettuare un trasferimento di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo o verso un'organizzazione internazionale, in forza di un obbligo previsto dal diritto dell'Unione europea o di uno Stato membro al quale è soggetto, ne informa tempestivamente il titolare prima di iniziare il trattamento, a meno che il diritto vieti di comunicare tale informazione per rilevanti motivi di interesse pubblico.

7. Designazione di un altro responsabile

Il responsabile non può ricorrere ad un altro responsabile (di seguito indicato come "sub-responsabile"), a meno del caso in cui ricorrano tutte le seguenti condizioni:

1. il responsabile abbia preventivamente comunicato per iscritto al titolare l'identità e i dati di contatto del sub-responsabile, le attività di trattamento ad esso affidate, la prova di quali garanzie siano state implementate, nonché i termini del contratto o atto giuridico che vincola il sub-responsabile ai medesimi obblighi previsti in capo al responsabile con il presente atto;
2. il responsabile abbia ottenuto dal titolare l'autorizzazione scritta, sia essa specifica o generale, del titolare. In caso di autorizzazione generale, la mancata opposizione da parte del titolare entro i successivi sette giorni lavorativi dalla ricezione della notifica scritta del Responsabile viene considerata come un'autorizzazione;
3. il responsabile abbia adottato garanzie sufficienti per implementare misure tecniche e organizzative adeguate tali da assicurare che il trattamento soddisfi i requisiti del Regolamento. In particolare, nel caso in cui il responsabile ricorra a un sub-responsabile stabilito in un Paese extra-UE, sarà suo onere adottare adeguati strumenti per legittimare il trasferimento ai sensi degli artt. 44 e ss. del Regolamento.

In tutti i casi, il responsabile rimane interamente responsabile nei confronti del titolare, qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati personali.
Il responsabile indica sin d'ora quali propri sub-responsabili i soggetti indicati *nel proprio sito Internet al seguente link _____ o mediante apposita comunicazione all'indirizzo PEC scriviunibo@pec.unibo.it*.

8. Obbligo di informare gli interessati

Scegliere una delle due opzioni:
[Opzione A]

È compito del titolare informare gli interessati in merito al trattamento effettuato sui dati personali dagli stessi forniti, al momento della loro raccolta e, qualora sia necessario, raccoglierne il relativo consenso al trattamento.
[Opzione B]
Il responsabile, al momento della raccolta dei dati personali, deve fornire agli interessati adeguate informazioni in merito al trattamento dei dati effettuato e, qualora sia previsto dalla legge, raccoglierne il relativo consenso. La formulazione e le modalità di fruizione dell'informativa e dell'eventuale modulo di acquisizione del consenso devono essere convenuti con il titolare, prima della raccolta dei dati.

9. Esercizio dei diritti degli interessati

Il responsabile deve assistere il titolare nell'adempimento dell'obbligo di evadere le richieste dell'interessato, qualora questi eserciti i diritti a lui attribuiti dalla vigente normativa in materia di protezione dei dati personali e, in particolare, dagli artt. 15- 21 del Regolamento, tra cui: il diritto di accesso, di rettifica, di cancellazione dei dati forniti; il diritto di opposizione e alla limitazione del trattamento; il diritto alla portabilità e il diritto a non essere soggetti a una decisione individuale automatizzata (compresa la profilazione).
Qualora gli interessati sottopongano al responsabile richieste per l'esercizio dei loro diritti, il responsabile deve inoltrare tali richieste non appena ricevute per e-mail all'indirizzo PEC del titolare *scriviunibo@pec.unibo.it* e alla casella di posta elettronica *privacy@unibo.it*.

10. Notifica di violazione di dati personali

[indicare nominativo del responsabile] comunica all'indirizzo *scriviunibo@pec.unibo.it*, nonché tramite posta elettronica semplice agli indirizzi: *rettore@unibo.it e dpo@unibo.it*, qualsiasi violazione dei dati personali[1] (c.d. *Data Breach*) entro e non oltre 24 ore dal momento in cui ne è venuto a conoscenza. Tale notifica deve essere corredata di tutta la documentazione necessaria per consentire al titolare, ove necessario, di notificare tale violazione all'autorità di vigilanza competente.
Il responsabile si impegna a prestare ogni necessaria collaborazione al titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle violazioni all'autorità di controllo competente (in Italia, il Garante per la protezione dei dati personali), ai sensi dell'art. 33 del Regolamento o nel caso di notifica della violazione agli interessati ai sensi dell'art. 34 del Regolamento.
La comunicazione al titolare conterrà almeno le seguenti informazioni:

- una descrizione dettagliata della violazione dei dati personali;
- la categoria di interessati e il tipo di dati che è stato oggetto di violazione dei dati personali e l'identità di ogni interessato (o, se non è possibile, il numero approssimativo delle persone interessate e i dati personali coinvolti);
- il nome e i contatti del proprio responsabile della protezione dei dati, o i recapiti di un altro punto di contatto attraverso cui è possibile ottenere ulteriori informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o che si intende adottare per affrontare la violazione dei dati personali, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi interventi attuati o che si prevede di attuare;
- non appena possibile, ogni altra informazione raccolta o resa disponibile, nonché ogni altra informazione che possa essere ragionevolmente richiesta dal titolare relativamente alla violazione dei dati personali.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il responsabile deve attivarsi immediatamente per indagare sulla violazione dei dati personali e per individuare, prevenire e limitare gli effetti negativi di tale violazione, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con il titolare, per svolgere qualsiasi

[1] È da considerarsi tale ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

azione che si renda necessaria per porre rimedio alla violazione stessa. Il responsabile non deve rilasciare, né pubblicare alcun comunicato stampa, avviso o relazione riguardante la violazione dei dati personali ("avvisi") senza aver ottenuto il previo consenso scritto del titolare.
Qualora la violazione dei dati personali tragga origine dalla mancata separazione di tipo logico dai dati personali trattati per conto di terze parti o per proprio conto di dati personali, le azioni e le procedure descritte nel presente articolo devono essere intraprese dal responsabile, senza che ciò pregiudichi il diritto del titolare di esercitare un qualsiasi rimedio giuridico a seguito della violazione.
Inoltre il responsabile dovrà pagare o rimborsare il titolare di tutti i costi, le perdite e le spese da quest'ultimo sostenute per la preparazione e pubblicazione degli avvisi.
Nel caso in cui la violazione dei dati personali avesse un impatto maggiore sui dati del responsabile, quest'ultimo dovrà comunque assicurare al titolare di poter agire nei tempi e nei modi indicati dalla legge e dal presente atto, anche assicurandogli priorità nel fornire il proprio supporto e nell'attuare i rimedi e le azioni che si riterranno necessarie.

11. Valutazione di impatto

Il responsabile s'impegna fin da ora a fornire al titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora lo stesso sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché a garantire la massima collaborazione nel caso in cui si renda necessario svolgere una consultazione preventiva all'autorità di controllo, ai sensi dell'art. 36 del Regolamento citato.

12. Misure tecniche e organizzative

Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura dell'oggetto del contesto, delle finalità del trattamento e del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile dovrà impegnarsi a garantire un livello di sicurezza dei dati e dei sistemi adeguato al rischio, attuando e garantendo le misure tecniche e organizzative richieste dal titolare. Il responsabile dovrà inoltre, in rapporto alle specifiche situazioni:

- Garantire la pseudonimizzazione e la cifratura dei dati personali;
- garantire la riservatezza, l'integrità, la disponibilità e la resilienza di sistemi e servizi di elaborazione;
- ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo nel caso di eventi che comportino un incidente fisico o tecnico;
- adottare procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In merito ai trattamenti effettuati senza l'ausilio di strumenti elettronici, il responsabile si impegna a:

- conservare gli atti e documenti cartacei contenenti dati personali in archivi o locali controllati, il cui accesso è limitato alle sole persone autorizzate al trattamento dei dati;
- custodire con diligenza gli atti e i documenti contenenti dati personali in maniera tale che le persone non autorizzate al trattamento non possano venirne a conoscenza, neppure accidentalmente (es. non lasciare documenti incustoditi sulla scrivania);
- evitare la duplicazione, laddove non strettamente necessaria, sia essa in forma elettronica o cartacea, di atti e documenti contenenti dati personali. In caso di duplicazione, conservare la copia cartacea o il supporto fisico su cui è memorizzata la copia in forma elettronica con le medesime modalità degli originali cartacei, al fine di assicurarne la riservatezza e integrità;
- qualora sia necessario distruggere atti e documenti contenenti dati personali, utilizzare appositi strumenti o modalità che ne impediscano il ricomponimento e il successivo utilizzo.

In merito ai trattamenti effettuati con l'ausilio di strumenti elettronici, il responsabile si impegna ad adottare almeno le misure di livello minimo di sicurezza individuate tra le "Misure minime di

sicurezza ICT per le pubbliche amministrazioni" (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015, pubblicante in GU n.103 del 05-05-2017). Inoltre, si impegna:

- ad adottare una procedura di autenticazione per accedere ai dispositivi informatici, attraverso "credenziali personalizzare di autenticazione", che consistono in un user-ID associato a una parola chiave segreta (password);
- ad assicurare che le credenziali di autenticazione siano utilizzate in modo pertinente e strettamente personale, non siano comunicate ad altri soggetti, neppure se parimenti autorizzati al trattamento, al fine di minimizzare i rischi di accesso illeciti e utilizzi impropri delle stesse;
- a prevedere un meccanismo di rinnovo della password almeno ogni sei mesi;
- a proteggere i sistemi informatici aziendali con strumenti idonei a garantire la sicurezza, l'integrità e la resilienza dei dispositivi, dei sistemi e della connessione utilizzata (es. attraverso l'installazione di firewall, software antivirus, ecc.);
- a predisporre procedure di aggiornamento periodico e automatico dei software di sicurezza installati sui diversi dispostivi;
- a prevedere meccanismi di pseudonimizzazione dei dati personali trattati, qualora non sia necessaria l'identificazione diretta del soggetto i cui dati si riferiscono;
- ad adottare una policy interna che definisca le modalità e le condizioni di utilizzo da parte del personale autorizzato dei dispositivi e dei sistemi informatici aziendali;
- a utilizzare un sistema di backup dei dati, al fine di evitare la perdita o la temporanea mancanza di accesso ai dati trattati.

Per tutte le misure di sicurezza sopra descritte, il responsabile si impegna a prevedere una procedura di riesame periodico delle misure di sicurezza adottate, con cadenza almeno annuale, al fine di procedere ad una loro rivalutazione e, se del caso, aggiornamento.

13. Audit

Il responsabile garantisce al titolare l'accesso ai propri locali, ai computer e ad altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il responsabile e/o i sub-responsabili rispettino gli obblighi disciplinati dal presente atto di nomina, sempre a condizione che tali verifiche non comportino l'analisi di tutti i dati di terze parti e che queste verifiche non collidano con obblighi di riservatezza del responsabile o del sub-responsabile.

14. Conservazione dei dati e conclusione del contratto

A discrezione del titolare, al termine della prestazione del servizio che comporta il trattamento dei dati personali di cui al presente atto, o qualora il titolare revochi la presente designazione o la stessa decada, il responsabile si impegna a:

- cancellare tutti i dati personali, comprese eventuali copie degli stessi, entro un congruo termine, in mancanza di termine comunicato dal titolare. Il responsabile deve eliminare tutte le copie esistenti dei dati, a meno che l'ulteriore archiviazione non sia richiesta da una norma di legge. Se il responsabile o il titolare è a conoscenza di tali requisiti legali, è tenuto a informare l'altra parte;
- restituire tutti i dati personali al titolare, entro un congruo termine, in mancanza di termine comunicato dal titolare;
- restituire i dati personali a un diverso responsabile designato dal titolare, entro un congruo termine, in mancanza di termine comunicato dal titolare.

La restituzione dei dati è accompagnata alla distruzione di tutte le copie cartacee e informatiche del responsabile. La distruzione dei dati deve essere documentata per iscritto dal responsabile. Sono fatti salvi i trattamenti eventualmente effettuati dal responsabile in qualità di titolare autonomo a norma di legge.

15. Responsabile della protezione dei dati personali

Il responsabile comunica al titolare il nome e i dati di contatto del proprio responsabile della protezione dei dati tramite PEC all'indirizzo *scriviunibo@pec.unibo.it*. Attualmente il ruolo è ricoperto da _____, email _____.

16. Registro delle attività di trattamento

Il responsabile dichiara di tenere per iscritto un registro di tutte le attività di trattamento effettuate per conto del titolare, ai sensi dell'art. 30, par. 2 del Regolamento, contenente tutte le informazioni ivi indicate.

17. Obblighi del titolare nei confronti del responsabile

Il titolare si impegna a:

- fornire al responsabile i dati descritti al par. 2 del presente atto;
- documentare per iscritto tutte le istruzioni concernenti il trattamento di dati, affidate al responsabile;
- vigilare e controllare il rispetto degli obblighi previsti dal Regolamento da parte del responsabile, nonché l'osservanza delle istruzioni ad esso fornite;
- supervisionare il trattamento, compresa l'effettuazione di attività di revisione e ispezioni presso il responsabile;
- mettere in atto le misure di sicurezza descritte nel paragrafo "Misure tecniche e organizzative" del presente atto, con riferimento alle strutture, agli strumenti e al personale dallo stesso impiegati per il trattamento dei dati personali, sottoposte al suo diretto controllo.

18. Adeguamento a nuove disposizioni

Le parti di comune accordo adegueranno le clausole contenute nel presente accordo al modello di atto giuridico e o clausole tipo predisposte dalla Commissione europea o da un'autorità di controllo per la disciplina del trattamento dei dati.
Durante l'esecuzione del contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di trattamento dei dati personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il responsabile si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

19. Durata

La presente designazione decorre dalla data in cui viene sottoscritta dalle parti ed è valida fino alla scadenza dei rapporti contrattuali richiamati all'art. 2 del presente atto, ovvero fino alla cessazione delle attività di elaborazione e di trattamento specificatamente richieste al responsabile.

20. Disposizioni finali

Resta inteso che la presente nomina non comporta alcun diritto per il responsabile a uno specifico compenso o indennità o rimborso per l'attività svolta, né a un incremento del compenso spettante allo stesso in virtù delle relazioni contrattuali con il titolare.
Per tutto quanto non previsto dal presente atto di nomina si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Data, *[indicare data della firma]*

Alma Mater Studiorum – Università di Bologna
Magnifico Rettore, Prof. Francesco Ubertini
(titolare del trattamento)
_____

Nome e cognome
(responsabile del trattamento)
_____