Prot. n. 0054724 del 02/05/2024 - [UOR: SI001070 - Classif. II/7]

ACCORDO DI CONTITOLARITÀ DEL TRATTAMENTO DEI DATI PERSONALI
***EX* ART. 26 DEL REGOLAMENTO (UE) 2016/679**

TRA

Università degli Studi di Messina, codice fiscale 80004070837 e partita IVA 00724160833 con sede a Messina, rappresentata dalla Magnifica Rettrice prof.ssa Giovanna Spatari (di seguito anche solo "**Unime**"),

E

Università degli Studi di Napoli Federico II, codice fiscale 00876220633 con sede a Napoli, rappresentata dal Magnifico Rettore prof. Matteo Lorito (di seguito anche solo "**Unina**"),

E

Università degli Studi "Magna Græcia" di Catanzaro, codice fiscale 97026980793 - partita IVA 02157060795 con sede in Viale Europa, Località Germaneto snc, 88100 Catanzaro, rappresentata dal Magnifico Rettore, Prof. Giovannni Cuda (di seguito anche solo "**Unicz**"),

e

Università degli Studi di Milano codice fiscale 80012650158 con sede a Milano, rappresentata dal Magnifico Rettore prof. Elio Franzini (di seguito anche solo "**Unimi**"),

di seguito, anche congiuntamente indicati come le "**Parti**" o i "**Contitolari**" e, singolarmente, come la "**Parte**"

PREMESSO CHE:

A. le Parti sono partner di un progetto di ricerca denominato "Furthering performance measurement systems in healthcare through new digital technologies" (di seguito anche solo il "progetto") il cui scopo è analizzare la diffusione, gli impatti e i fattori che influenzano l'introduzione delle nuove tecnologie digitali (AI, IoT, Machine learning, Big Data analytics, Social media, blockchain, cloud computing, ecc.) nei servizi amministrativi e gestionali delle Aziende Sanitarie e, in particolare, nei sistemi di performance measurement e management;

B. l'attività di ricerca comporta la raccolta di dati personali, così come definiti dall'art. 4 del Regolamento (UE) 2016/679 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 (di seguito, il "**Regolamento**") e precisamente la raccolta dei dati appartenenti alle categorie meglio individuate nell'allegato 1 di questo accordo (di seguito l'"**Allegato 1**"), relative ai soggetti partecipanti alla ricerca (di seguito gli "**Interessati**") anch'essi meglio individuati nell'Allegato 1;

C. in virtù di quanto indicato, con il presente accordo (di seguito l'"**Accordo**") le Parti intendono dunque regolare il rapporto di contitolarità nel trattamento dei dati personali relativi agli Interessati, e disciplinare, di conseguenza, i rispettivi ruoli e responsabilità nei confronti degli Interessati;

D. nell'ambito delle rispettive responsabilità come determinate dal presente Accordo, le Parti dovranno in ogni momento adempiere ai propri obblighi conformemente ad esso e in modo tale da trattare i dati senza violare le disposizioni di legge vigenti e nel pieno rispetto delle

linee guida e dei codici di condotta applicabili di volta in volta approvati dal Garante per la protezione dei dati personali.

TUTTO CIÒ PREMESSO, LE PARTI STIPULANO E CONVENGONO QUANTO SEGUE.

1. OGGETTO

1.1. Le premesse sono parte integrante e sostanziale del presente accordo.

1.2. Con il presente Accordo le Parti: ***(i)*** definiscono termini e modalità che si impegnano ad attuare per effettuare le operazioni di trattamento dei dati personali meglio definiti nell'Allegato 1; ***(ii)*** determinano le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, nonché dalle disposizioni di legge vigenti con riguardo al trattamento dei dati personali relativi agli Interessati; e ***(iii)*** stabiliscono i rispettivi obblighi in merito all'esercizio dei diritti degli Interessati.

1.3. La contitolarità è riferita al trattamento dei dati personali, come definiti al punto B delle premesse e meglio individuati nell'Allegato 1. Le finalità e le modalità con le quali si procede al trattamento congiunto sono ugualmente individuate e meglio descritte nell'Allegato 1.

1.4. I termini "Titolare del trattamento", "Responsabile del trattamento", "consenso", "pseudonimizzazione", "dati personali", "trattamento", "violazione dei dati personali", hanno nell'Accordo lo stesso significato che hanno nel Regolamento. Per "Paesi terzi" si intendono tutti i Paesi che non sono Stati membri dell'Unione Europea e/o che non rientrano nell'ambito di applicazione delle leggi sulla protezione dei dati dello Spazio Economico Europeo ("SEE").

2. OBBLIGHI DEI CONTITOLARI ED ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

2.1. I Contitolari condividono le modalità del trattamento dei dati personali relativi agli Interessati raccolti nell'ambito del progetto e sono obbligati in solido a predisporre e mantenere aggiornati tutti gli adempimenti previsti dal Regolamento e dalle disposizioni di legge vigenti in materia di tutela dei dati personali.

2.2. Ciascuna parte, per quanto di propria competenza, individuerà, istruirà e autorizzerà per iscritto le persone che, sotto la propria autorità, tratteranno i dati Personali nell'esecuzione del presente accordo.

2.3. Qualora per i trattamenti oggetto del presente contratto una Parte ritenga necessario avvalersi dei servizi di terzi fornitori dai quali possa derivare il trattamento di dati personali oggetto di contitolarità, la stessa si impegna a darne notizia alle altre Parti, avendo cura di fornire informazioni sufficienti sul trattamento e sui trattamenti che saranno effettuati avvalendosi del servizio di terzi e sulle misure tecniche ed organizzative per la tutela dei dati personali adottate dal fornitore. Ai fini dell'affidamento dei trattamenti al terzo fornitore è necessario acquisire il consenso scritto di tutte le Parti del presente contratto. Le Parti si impegnano a negoziare in buonafede gli accordi per la nomina a Responsabile dei terzi fornitori, avendo cura di rispettare le prescrizioni di cui all'art. 28 del Regolamento. I Responsabili del trattamento indicati nell'Allegato 1 si intendono come noti, valutati ed accettati da tutte le Parti, anche laddove la nomina a Responsabile dovesse essere siglata da una sola di esse a nome e per conto di tutte.

2.4. Le Parti convengono di individuare un punto di contatto per gli Interessati, ai sensi dell'art. 26, comma 1, del Regolamento, al quale viene attribuito altresì l'incarico di fornire agli interessati il foglio informativo relativo alla ricerca e l'informativa per il trattamento dei dati personali, raccogliendo i relativi consensi (ove richiesti). Sarà cura del punto di contatto conservare altresì l'originale firmato del foglio informativo, dell'informativa per il trattamento dei dati personali e dei moduli di acquisizione del consenso. La Parte che fungerà da punto di contatto viene individuata nell'Allegato 1.

2.5. Fermo restando l'art. 26, comma 3, del Regolamento, Le Parti convengono inoltre che gli Interessati eserciteranno i propri diritti rivolgendosi al punto di contatto meglio individuato nell'Allegato 1, il quale gestirà la richiesta coinvolgendo, laddove necessario, le altre Parti. Tutte le Parti si impegnano sin da ora a fornire a quest'ultima tutto il supporto, anche

tecnico, necessario per evadere tempestivamente ogni richiesta presentata dagli Interessati o dall'Autorità Garante.

2.6. Le Parti si impegnano altresì, ai sensi dell'art. 26, comma 2, del Regolamento, a mettere a disposizione dell'Interessato il contenuto essenziale del presente Accordo qualora richiesto. I recapiti di tutte le Parti sono meglio individuati nell'Allegato 1.

2.7. Le attività di trattamento demandate a ciascuna delle Parti e che esulano dal progetto restano di singola competenza di ciascuna Parte, la quale agirà quale autonomo titolare del trattamento, salvo che intervenga un ulteriore accordo di contitolarità.

2.8. Le Parti non rilasceranno alcun dato personale a terzi, fatta eccezione per le situazioni di seguito individuate:
- quando è previsto il trattamento da parte di Responsabili del trattamento approvati ai sensi del precedente punto 2.3;
- se richiesto dalla legge. Nel caso in cui una delle Parti sia costretta da un'autorità giudiziaria o amministrativa a trasferire i dati elaborati, a maggior ragione se l'obbligo di trasferimento dovesse riguardare un paese diverso dall'Italia o un'organizzazione internazionale, dovrà informare immediatamente le altre Parti di tale obbligo legale, a meno che la legge in questione non vieti espressamente tale divulgazione sulla base di significative considerazioni di interesse pubblico.

2.9. Qualsiasi trattamento di dati personali effettuato in un Paese Terzo o in un'organizzazione internazionale ai sensi del presente Accordo di trattamento da una delle Parti comporterà l'imposizione di garanzie adeguate che assicurino un livello di protezione equivalente a quello previsto dagli articoli da 44 a 50 del Regolamento e dovrà essere approvato da ciascuna Parte.

2.10. Su richiesta di una delle Parti, ciascuna Parte fornirà la documentazione necessaria a dimostrare il rispetto di tutti gli obblighi previsti da questo Accordo e in particolare dagli artt. 2 e 3.

2.11. L'Autorità di Vigilanza competente può effettuare controlli presso una o più Parti. In caso di ispezione, la Parte o le Parti interessate si informano vicendevolmente delle informazioni richieste dall'Autorità di Vigilanza e, se del caso, delle risposte fornite a quest'ultima; ciascuna Parte agisce in conformità alle richieste di detta autorità.
Le Parti si consultano reciprocamente per fornire tutte le informazioni e i documenti richiesti dall'Autorità di Vigilanza.
In ogni caso, la Parte sottoposta a verifica comunicherà il presente Accordo di trattamento all'Autorità di Vigilanza, se richiesto.

3. SICUREZZA DELLE INFORMAZIONI

3.1. Ciascuna Parte è tenuta a mettere in atto e mantenere per tutta la durata del presente Accordo tutte le misure di sicurezza tecniche e organizzative adeguate per proteggere i dati personali raccolti, trattati o utilizzati nell'ambito del rapporto di contitolarità da accessi non autorizzati o illegali, divulgazione, alterazione, perdita o distruzione accidentale, in conformità a quanto previsto dall'art. 32 del Regolamento, nonché per garantirne accuratezza e completezza per tutta la durata del trattamento.
Tali misure devono comprendere:
(i) l'impedimento all'accesso ai sistemi di trattamento dei dati personali da parte di persone non autorizzate (controllo dell'accesso fisico);
(ii) l'impedimento all'uso non autorizzato dei sistemi di trattamento dei dati personali (controllo dell'accesso logico);
(iii) la garanzia che le persone autorizzate a utilizzare un sistema di trattamento dei dati personali abbiano accesso solo ai dati personali a cui sono autorizzate ad accedere in base ai loro diritti di accesso. Durante il trattamento, tali dati personali non devono essere letti, copiati, modificati o cancellati senza autorizzazione (controllo dell'accesso ai dati);
(iv) la garanzia che i dati personali raccolti siano protetti contro la distruzione o la perdita accidentale (verifica della disponibilità);
(v) la garanzia che i dati personali trattati siano elaborati solo in conformità alle istruzioni (controllo delle istruzioni).

A questo fine tutte le Parti allegano al presente accordo una sintesi delle misure di sicurezza in uso presso le proprie organizzazioni/strutture (Allegati 2).

3.2. Le Parti adegueranno sistematicamente le misure adottate all'evoluzione della normativa, della tecnologia e di altri aspetti. In ogni caso, le misure tecniche e organizzative implementate devono garantire un livello di sicurezza adeguato in relazione ai rischi associati al Trattamento e alla natura dei Dati personali da proteggere. Ciò tiene conto anche del progresso delle tecnologie e del costo della loro implementazione.
Per tutta la durata dell'Accordo sul trattamento, ciascuna Parte informerà per iscritto l'altra o le altre Parti di qualsiasi modifica agli allegati che descrivono le misure di protezione tecniche e organizzative applicate.

3.3. Ciascuna Parte adotterà tutte le misure di sicurezza tecniche e organizzative necessarie ai fini del tempestivo recupero della disponibilità dei dati personali in caso di incidente fisico o tecnico.

3.4. Nell'ipotesi di una violazione dei Dati Personali ("Data Breach"), o di sospetta violazione dei dati personali, la Parte interessata informerà senza indugio le altre Parti di quanto occorso e delle potenziali conseguenze, entro 12 ore e comunque tenendo conto del periodo di 72 ore previsto dal GDPR per la notifica della violazione all'autorità di vigilanza.
Tali informazioni saranno fornite:
1) all'indirizzo individuato da ciascuna parte per le comunicazioni e indicato nell'Allegato 1
2) al/ai responsabile/i della protezione dei dati o ai rappresentanti incaricati della protezione dei dati i cui dati di contatto sono elencati nell'Allegato 1.
La Parte nei cui locali o nella cui infrastruttura informatica si è verificata la violazione dei dati personali dovrà indagare sulla violazione nel più breve tempo possibile. Essa tiene informata le altre Parti dei progressi dell'indagine e adotta misure ragionevoli per attenuarne le conseguenze. Tutte le Parti convengono sin da ora di cooperare pienamente nelle indagini sul Data Breach e si impegnano ad assistersi reciprocamente nell'adempimento di eventuali obblighi di notifica.
L'obbligo di una Parte di segnalare o rispondere a una violazione dei dati personali non è e non deve essere interpretato come un'ammissione da parte di tale Parte di qualsiasi colpa o responsabilità in relazione a tale violazione.
Ciascuna Parte sarà separatamente responsabile della notifica di una violazione dei dati personali all'Autorità di Vigilanza competente e/o agli Interessati se la violazione dei dati personali si è verificata sotto la propria responsabilità. Le Parti si terranno reciprocamente informate, se del caso, di tali notifiche e del loro contenuto.
Ciascuna Parte è tenuta, per quanto possibile, a porre rimedio alle conseguenze negative di tali violazioni e/o a ridurre al minimo qualsiasi altra conseguenza. Ciascuna parte dovrà attuare con diligenza e senza indugio i rimedi richiesti dalle Autorità di Vigilanza competenti per far fronte a qualsiasi violazione dei dati personali, ad altre inadempienze e/o per mitigare i rischi correlati. Le Parti si terranno reciprocamente informate sugli ultimi sviluppi relativi alla violazione dei dati personali. Qualora si debbano sostenere dei costi per cercare di risolvere la situazione di violazione e garantire che non si verifichi in futuro, tali costi saranno sostenuti dalla Parte nei cui locali si è verificata la violazione dei dati. Le Parti si riservano comunque di prendere in considerazione la possibilità di condividere i costi se la soluzione va a vantaggio di tutte le Parti partecipanti.

3.5. Se, in virtù della sua natura, del volume dei dati, del contesto e della finalità prevista, un'operazione di trattamento dei dati dovesse anche solo astrattamente presentare un rischio elevato per i diritti e le libertà delle persone fisiche, le Parti effettueranno una valutazione d'impatto sulla protezione dei dati (**"DPIA"**) sull'operazione di trattamento dei dati in esame, assicurando una stretta collaborazione tra loro.

3.6. Le Parti potranno conservare i dati per il periodo indicato nell'Allegato 1.

4. RESPONSABILITÀ E COMUNICAZIONI TRA LE PARTI

4.1. I Contitolari di cui al presente Accordo di contitolarità congiuntamente determinano di ripartire tra di essi la responsabilità derivante da eventuali danni arrecati agli Interessati e a soggetti terzi in ragione delle rispettive attività definite nell'art. 1.2, 1.3, 2.1, 2.2, 2.3,

2.4, 2.5, 2.6, 2.8, 2.9, 2.10., 2.11, 3.1, 3.2, 3.3, 3.4, 3.5 e 3.6 del presente Accordo. Nessun Contitolare sarà quindi da considerarsi responsabile nel caso in cui il danno occorso sia imputabile, direttamente o indirettamente, all'attività svolta da altro Contitolare. E' fatta salva, in ogni caso, la possibilità per quest'ultimo di esercizio del diritto di regresso ai sensi dell'art. 82 c. 5 del GDPR.

4.2. Ciascun Contitolare si impegna a comunicare tempestivamente agli altri Contitolari qualsiasi richiesta, ispezione, controllo o provvedimento da parte dell'Autorità Garante o dell'Autorità Giudiziaria, ovvero citazione in giudizio che dovesse pervenire relativamente al trattamento dei dati personali oggetto del presente Accordo.

4.3. Le Parti, salvo diversa specifica previsione contenuta nell'Accordo, stabiliscono che qualsiasi comunicazione o notifica richiesta o consentita dall'Accordo dovrà essere effettuata per iscritto, a mezzo PEC. Dette comunicazioni o notifiche si considereranno perfezionate nella data in cui la Parte che abbia inviato la comunicazione o la notifica ottenga una regolare conferma di trasmissione al destinatario. Le comunicazioni e le notifiche dovranno essere indirizzate agli indirizzi di posta elettronica certificata meglio individuati nell'Allegato 1.

5. DURATA DELL'ACCORDO E DIVIETO DI CESSIONE

5.1. Il presente Accordo sarà efficace sino al completamento del progetto, fatto salvo un successivo diverso accordo tra le Parti.

5.2. Restando inteso che in ipotesi di cessazione del progetto per qualsivoglia ragione intervenuta, il presente Accordo cesserà di produrre effetto tra le Parti a far data dalla data di cessazione dello studio/progetto medesimo.

5.3. È fatto espresso ed assoluto divieto alle Parti di cedere, in tutto o in parte, il presente Accordo e/o i diritti e gli obblighi da esso derivanti.

5.4. Qualsiasi modifica di questo Accordo e dell'Allegato 1 sarà valida ed efficace tra le Parti solo se in forma scritta e redatta nelle forme dell'emendamento.

6. LEGGE APPLICABILE E FORO COMPETENTE

6.1. Il presente Accordo è regolato dalla legge italiana e dovrà essere interpretato ai sensi e per gli effetti della medesima.

6.2. Ogni e qualsiasi controversia relativa all'interpretazione e/o alla validità e/o all'efficacia e/o all'esecuzione del presente Accordo, sarà devoluta alla competenza esclusiva del Foro di Milano.

7. CLAUSOLE VESSATORIE

7.1. Le Parti espressamente dichiarano che tutte le disposizioni del presente Accordo sono state oggetto di negoziazione tra di esse e che, pertanto, non trovano applicazione gli artt. 1341 e 1342 c.c.

UNIVERSITA' DEGLI STUDI DI MILANO

Elio Franzini
Universita' degli Studi di Milano
04.04.2024 05:52:44
GMT+00:00

Il Rettore
Prof. Elio Franzini

UNIVERSITA' DEGLI STUDI DI MESSINA

La Rettrice
Prof.ssa Giovanna Spatari

UNIVERSITA' DEGLI STUDI FEDERICO II DI NAPOLI

Firmato digitalmente da
Matteo LORITO
CN = LORITO Matteo
O = Universita' degli Studi di Napoli Federico II
C = IT

Il Rettore
Prof. Matteo Lorito

UNIVERSITA' DEGLI STUDI DELLA MAGNA GRAECIA DI CATANZARO

Il Rettore
Prof. Giovanni Cuda

Allegato 1

DESCRIZIONE DEI TRATTAMENTI CONGIUNTI POSTI IN ESSERE DALLE PARTI

1. Tipologie di dati personali che dovranno essere trattati

Le categorie di dati personali in forma grezza che saranno raccolti e trattati da ciascun contitolare sono quelle di seguito meglio specificate:

(i) Dati identificativi (nome, cognome, azienda di appartenenza)

(ii) fascia d'età;

(iii) sesso;

(iv) anni totali nel ruolo considerato;

(v) anni totali in azienda;

(vi) anni di esperienza complessivi nelle aziende sanitarie;

(vii) anni di esperienza complessivi con il ruolo considerato;

(viii) titolo di studio;

(ix) background formativo;

(x) opinioni personali e professionali sugli argomenti oggetto di survey;

(xi) recapiti.

Le categorie di dati personali che saranno trasferite in esecuzione del presente contratto sono:

(xii) dati identificativi (nome, cognome, azienda di appartenenza)

(i) fascia d'età;

(ii) sesso;

(iii) anni totali nel ruolo considerato;

(iv) anni totali in azienda;

(v) anni di esperienza complessivi nelle aziende sanitarie;

(vi) anni di esperienza complessivi con il ruolo considerato;

(vii) titolo di studio;

(viii) background formativo;

(ix) opinioni personali e professionali sugli argomenti oggetto di survey;

(x) recapiti.

2. Categorie di interessati

Gli interessati saranno soggetti che ricoprono i seguenti ruoli all'interno di aziende sanitarie pubbliche (ASL, ATS, ASST, AO, AOU, IRCCS e Fondazioni IRCCS) e aziende sanitarie private sul territorio italiano: Direttori generali (e/o Amministratori Delegati), Direttori amministrativi, Chief Information Officer (o Direttori dei Servizi Informativi), Direttori del servizio Programmazione e Controllo.

3. Finalità perseguite

La finalità del trattamento è quella di conseguire l'obiettivo che il progetto si propone, ovvero analizzare la diffusione, gli impatti e i fattori che influenzano l'introduzione delle nuove tecnologie digitali (AI, IoT, Machine learning, Big Data analytics, Social media, blockchain, cloud computing, ecc.) nei servizi amministrativi e gestionali delle Aziende Sanitarie e, in particolare, nei sistemi di performance measurement e management.

4. Tipologie di trattamento che si prevede di effettuare

Raccolta dei dati – Unimi, Unime, Unina, Unicz raccoglieranno dati empirici utilizzando strumenti di survey standardizzati per la raccolta dei dati per i quali è stata effettuata una verifica di privacy compliance da parte di Unimi (EU Survey; Lime Survey disattivando Google Analytics, Survey Monkey con piano a pagamento; Question Pro con richiesta esplicita di conservazione dei dati entro lo spazio economico europeo; Qualtrics disattivando la funzione di installazione di codici per la generazione di Google Analytics; Microsoft Forms). In ogni caso saranno adottati tutti gli accorgimenti resi disponibili dai software per minimizzare il trattamento dei dati personali dei compilanti). Le survey saranno indirizzate ai soggetti interessati di cui al punto 2, ed inviate agli indirizzi di posta elettronica istituzionali non nominativi reperiti sulle pagine web delle aziende sanitarie pubbliche e private. I dati grezzi saranno acquisiti attraverso le risposte fornite alle domande chiuse della survey; i medesimi saranno successivamente sottoposti ad una serie di analisi volte a (i) descrivere lo stato dell'arte della diffusione delle nuove tecnologie digitali nelle aziende sanitarie, degli impatti e dei fattori che ne influenzano l'adozione; (ii) registrare le percezioni sulle nuove tecnologie digitali nelle aziende sanitarie e confronto delle diverse percezioni a seconda di ruolo, tipologia di azienda, posizione geografica (nord ovest, nord est, centro, sud e isole), background formativo, anni in ruolo, ecc.; (iii) individuare un legame tra lo stato dell'arte dell'adozione delle tecnologie e le caratteristiche dei rispondenti (dati personali) e delle relative aziende a cui essi afferiscono; (iv) individuare il legame tra le variabili colte dalla survey ed ulteriori variabili successivamente collezionate (ad es. finalizzate ad individuare un legame con dati di performance aziendale).
Unimi, Unime, Unina, UniCZ raccoglieranno altresì dati pubblici sulle aziende coinvolte e sui soggetti che ricoprono gli incarichi presi in esame per il progetto ricorrendo ai portali messi a disposizione dalla Pubblica Amministrazione (siti web di Agenas, Ministero delle Finanze, Ministero della Salute, Ministero dell'Università e della Ricerca, SSR e Agenzie Sanitarie Regionali, Aziende Sanitarie Pubbliche, ecc.) e dalle Aziende Sanitarie Private, anche per il tramite di associazioni e federazioni di categoria (AIOP, FIASO, FEDERSANITA', ecc.).
Pseudonimizzazione dei dati – tutte le Parti provvederanno, come misura di sicurezza, a pseudonimizzare i dati degli interessati ricorrendo alla associazione dei nominativi con codici e valuteranno l'adozione di codici o di altre misure di minimizzazione anche per gli altri elementi (es: professione, Azienda sanitaria di appartenenza, informazioni sul

background) che potrebbero consentire agevolmente l'identificazione degli Interessati, in particolare se associati ai dati disponibili pubblicamente.
Trasmissione dei dati – Le parti si trasmetteranno vicendevolmente e si comunicheranno dati preferibilmente pseudonimizzati. I file da trasmettere saranno cifrati alla fonte e poi trasmessi tramite canali utili allo scopo (email, utilizzo di dispositivi mobili quali chiavette USB, Microsoft Teams, che ha un sistema di cifratura di default su file condivisi) senza chiave di cifratura e/o identificazione, che sarà comunicata separatamente. Nel caso in cui si decida di optare per dispositivi mobili come le chiavette USB, queste dovranno a loro volta essere cifrate. In ogni caso, a trasmissione avvenuta ed esaurita la finalità del trattamento, verrà richiesto di eliminare la copia dei documenti salvati sullo strumento utilizzato per la trasmissione (es. eliminando il messaggio di posta elettronica con il documento in allegato, ovvero eliminando o limitando ulteriormente gli accessi ai file salvati sulle cartelle cloud condivise). Nell'ipotesi di utilizzo di Microsoft Teams, Microsoft si configura come Responsabile del trattamento ai sensi dell'art. 28 GDPR, come meglio dettagliato nell' Addendum relativo alla Protezione dei Dati Personali dei Prodotti e dei Servizi Microsoft (versione 1° gennaio 2023) sottoscritto e accettato da tutti i contitolari.
Conservazione dei dati – Ciascuna delle parti memorizzerà separatamente i dati grezzi raccolti e i codici di identificazione nei propri database; i file (sia quelli contenenti i dati grezzi, sia quelli contenenti i codici di reidentificazione) saranno protetti da apposita password e conservati nei computer dei propri ricercatori protetti da password. Le due serie di dati dovranno essere conservate in modo tale che nessuna persona o tecnologia possa facilmente metterle in collegamento e procedere all'accesso ai dati e/o alla identificazione degli Interessati. I dati saranno conservati per 5 anni; la fase di raccolta dei dati terminerà entro il termine previsto per la conclusione del progetto. Il PRIN 2022 ha durata di 2 anni a partire dal 28 settembre 2023.
Consultazione dei dati – Ciascuna delle Parti può consultare dati pseudonimizzati (ulteriori rispetto a quelli elencati al punto 1 del presente allegato) di cui non dispone e che sono conservati presso altra Parte previa richiesta scritta motivata e approvazione della Parte detentrice e del coordinatore del Progetto.
Anonimizzazione dei dati – Durante l'anonimizzazione dei dati, cinque anni dopo la fine della fase di raccolta, tutte le parti cancelleranno i dati grezzi raccolti (nominativi di chi ha partecipato al progetto e risposte alle survey). Questo processo irreversibile renderà le persone non più identificabili da nessuno, in linea con il considerando 26 del regolamento (UE) 2016/679.

5. Basi giuridiche del trattamento

La base giuridica del trattamento è il consenso dell'interessato ai sensi dell'articolo 6, paragrafo 1, lettera a del Regolamento (UE) 2016/679. Il consenso dell'interessato è espresso tramite azione positiva inequivocabile (flag nella pagina dedicata prima dell'inizio del questionario).

6. Responsabile della protezione dei dati o rappresentante incaricato della protezione di dati personali

Per Università degli Studi di Milano: DPO Prof. Avv. Pierluigi Perri (dpo@unimi.it)
Per Università degli Studi di Messina: DPO Dott.ssa Daniela Prestipino (dpo@unime.it)
Per Università degli Studi Napoli Federico II: Dott.ssa Avv. Gabriella Formica (rpd@unina.it)
Per Università degli Studi Magna Græcia di Catanzaro: DPO Dott. Stefano Ruffolo (dpo@unicz.it)

7. Responsabili del trattamento

Al momento le Parti hanno individuato i seguenti Responsabili del trattamento, per i quali è già stato sottoscritto o è in corso di sottoscrizione uno specifico accordo ai sensi dell'art. 28 del Regolamento:

Ragione sociale Responsabile	Attività demandata (in sintesi)
Microsoft Ireland Operations, Ltd.	Erogazione di servizi online, con particolare riferimento all'applicazione di collaborazione per il lavoro ibrido (Teams)

8. Termini di durata della conservazione dei dati personali

I dati saranno conservati per 5 anni; la fase di raccolta dei dati terminerà entro il termine previsto per la conclusione del progetto. Il PRIN 2022 ha durata di 2 anni a partire dal 28 settembre 2023. Tutte le Parti in possesso di chiave di identificazione dei dati pseudonimizzati provvederanno a cancellarle in modo che i dati pseudonimizzati trasmessi inizialmente alle istituzioni coordinatrici del Work Package e al coordinatore generale del progetto siano completamente anonimizzati. Saranno ugualmente pseudonimizzati (senza conservazione della chiave di identificazione) o anonimizzati gli altri dati, anche non personali, idonei a consentire una agevole identificazione degli interessati, da soli o associati a dati pubblici. Le risposte fornite alle survey, ove non già aggregate per gli scopi del Progetto, saranno eliminate.

9. Punto di contatto e recapiti delle Parti per l'esercizio dei diritti da parte degli interessati

Stante la tipologia di ricerca, la natura e il numero di interessati coinvolti, le Parti convengono di non individuare un unico punto di contatto. Sarà pertanto facoltà degli interessati rivolgersi a tutti o ciascuno dei contitolari ai seguenti recapiti:
Per Università degli Studi di Milano: via Festa del Perdono n. 7 20122 Milano – PEC: unimi@postacert.it - DPO Prof.Avv. Pierluigi Perri (dpo@unimi.it)
Per Università degli Studi di Messina: piazza Pugliatti n. 1 98121 Messina – PEC: protocollo@pec.unime.it -DPO Dott.ssa Daniela Prestipino (dpo@unime.it)
Per Università degli Studi Napoli Federico II: Corso Umberto I n. 40 80138 Napoli - PEC: ateneo@pec.unina.it – DPO Dott.ssa Avv. Gabriella Formica (rpd@unina.it)
Per Università degli Studi Magna Græcia di Catanzaro: Viale Europa snc - Località Germaneto 88100 Catanzaro – PEC: protocollo@cert.unicz.it - DPO Dott. Stefano Ruffolo (dpo@unicz.it)

Allegato 2 a)

MISURE TECNICHE ED ORGANIZZATIVE IN USO PRESSO UNIVERSITA'DEGLI STUDI DI MILANO

Misure Tecniche

☒ Misure di protezione delle singole apparecchiature informatiche (antivirus, aggiornamenti e patch di sicurezza, test, ecc.).
☒ Misure di protezione fisica dei locali e delle apparecchiature (accesso tramite chiave o codice o badge; elenco aggiornato delle persone autorizzate; registro dei visitatori; videosorveglianza; allarme, ecc.).
☒ Misure di protezione logica per l'accesso alle apparecchiature, ai server e ai dati (accesso con identificatore unico e meccanismo di autenticazione, ecc.).
☒ Misure strutturali per il backup e la disponibilità dei dati.
☒ Misure per la crittografia dei supporti di memorizzazione dei dati.
☒ Misure di crittografia per il trasferimento dei dati.
☐ Misure che assicurano una maggiore pseudonimizzazione delle informazioni in ambienti di test.
☒ Gestione completa del ciclo degli account (utenti, amministratori, account tecnici) e delle autorizzazioni (dalla creazione alla chiusura, incluse le sospensioni).
☒ Restrizione e controllo dell'accesso a locali, apparecchiature e dati in base a permessi/funzioni ("need-to-know").
☒ Misure di tracciabilità: registrazione dell'accesso dell'utente all'ambiente (tracciamento delle connessioni locali e remote), dati registrati (ad es. login, data e ora della connessione, ecc.) e periodo di conservazione.
☒ Sistema di prevenzione e rilevamento delle intrusioni di rete.
☒ Misure di gestione delle vulnerabilità tecniche (rilevamento, patching, ecc.).
☒ Telecamere di sicurezza all'ingresso dei locali.
☐ Controllo e gestione dei supporti rimovibili per prevenire la divulgazione, la modifica, la cancellazione o la distruzione non autorizzata di dati personali.
☒ Dispositivi di archiviazione sicuri per proteggere i registri e le apparecchiature e prevenire la perdita, il danneggiamento, il furto o la messa in pericolo dei dati personali.
☐ Altro (specificare):

Misure organizzative

☒ Politica di sicurezza del sistema informativo e politica di protezione dei dati (scenario di violazione dei dati, procedura di arrivo e partenza del personale, best practice ICT, ecc.).
☒ Sensibilizzazione e formazione del personale e dei collaboratori esterni coinvolti nel trattamento dei dati personali.
☒ Nomina di un responsabile della protezione dei dati o di un responsabile della gestione della protezione dei dati (DPO).
☒ Nomina di un responsabile della sicurezza informatica.
☒ Organigramma interno e chiara suddivisione dei compiti.
☒ Personale vincolato dal segreto professionale o da un accordo di riservatezza.

☒ Prevenzione, individuazione e trattamento dei rischi fisici (incendi, danni da acqua, ecc.).
☒ Processo di cancellazione sicura dei dati (ad es. distruggidocumenti, ecc.).
☒ Piano di ripristino, di disastro o di emergenza (piano di continuità operativa e di ripristino).
☒ Procedura di gestione degli incidenti di sicurezza.
☒ Registro degli incidenti in relazione al monitoraggio operativo dell'elaborazione.
☒ Audit periodico dell'ambiente, delle soluzioni e delle procedure.
☒ Misure di informazione per gli interessati (informativa sulla privacy, politica sui cookie nei siti e/o nelle web-app, ecc.).
☐ Altro (specificare):

Allegato 2 b)

MISURE TECNICHE ED ORGANIZZATIVE IN USO PRESSO UNIVERSITA'DEGLI STUDI DI MESSINA

Misure Tecniche

☐ Misure di protezione delle singole apparecchiature informatiche (antivirus, aggiornamenti e patch di sicurezza, test, ecc.).
☐ Misure di protezione fisica dei locali e delle apparecchiature (accesso tramite chiave o codice o badge; elenco aggiornato delle persone autorizzate; registro dei visitatori; videosorveglianza; allarme, ecc.).
☐ Misure di protezione logica per l'accesso alle apparecchiature, ai server e ai dati (accesso con identificatore unico e meccanismo di autenticazione, ecc.).
☐ Misure strutturali per il backup e la disponibilità dei dati.
☐ Misure per la crittografia dei supporti di memorizzazione dei dati.
☐ Misure di crittografia per il trasferimento dei dati.
☐ Misure che assicurano una maggiore pseudonimizzazione delle informazioni in ambienti di test.
☐ Gestione completa del ciclo degli account (utenti, amministratori, account tecnici) e delle autorizzazioni (dalla creazione alla chiusura, incluse le sospensioni).
☐ Restrizione e controllo dell'accesso a locali, apparecchiature e dati in base a permessi/funzioni ("need-to-know").
☐ Misure di tracciabilità: registrazione dell'accesso dell'utente all'ambiente (tracciamento delle connessioni locali e remote), dati registrati (ad es. login, data e ora della connessione, ecc.) e periodo di conservazione.
X Sistema di prevenzione e rilevamento delle intrusioni di rete.
☐ Misure di gestione delle vulnerabilità tecniche (rilevamento, patching, ecc.).
☐ Telecamere di sicurezza all'ingresso dei locali.
☐ Controllo e gestione dei supporti rimovibili per prevenire la divulgazione, la modifica, la cancellazione o la distruzione non autorizzata di dati personali.
☐ Dispositivi di archiviazione sicuri per proteggere i registri e le apparecchiature e prevenire la perdita, il danneggiamento, il furto o la messa in pericolo dei dati personali.
X Altro (specificare): **Per i servizi cloud (Microsoft Azure) è attiva la Multifactor Authentication che è obbligatoria per gli amministratori ed attualmente facoltativa per tutto il resto degli utenti.**
Le seguenti misure tecniche non sono selezionate in quanto non sono applicate globalmente per tutta l'organizzazione:

- **Misure di protezione delle singole apparecchiature informatiche (antivirus, aggiornamenti e patch di sicurezza, test, ecc.).**

  Sono attive sui servers centrali in gestione al CIAM e sugli endpoint in uso al PTA gestiti centralmente

- **Misure di tracciabilità: registrazione dell'accesso dell'utente all'ambiente (tracciamento delle connessioni locali e remote), dati registrati (ad es. login, data e ora della connessione, ecc.) e periodo di conservazione.**

  Sono presenti nelle applicazioni e server gestiti centralmente dal CIAM e nei servizi in SSO

- **Misure di protezione fisica dei locali e delle apparecchiature (accesso tramite chiave o codice o badge; elenco aggiornato delle persone autorizzate; registro dei visitatori; videosorveglianza; allarme, ecc.).**

  Per la sala macchine CIAM sono presenti misure di protezione fisica. L'accesso è personale tramite apposite credenziali, ed è presente un sistema di videosorveglianza. Tale misura non è selezionata in quanto non omogenea per le altre aree decentrate dell'Ateneo.

  I racks della rete di Ateneo dislocati nell'organizzazione sono protetti da serratura.

- **Misure di protezione logica per l'accesso alle apparecchiature, ai server e ai dati (accesso con identificatore unico e meccanismo di autenticazione, ecc.).**

  E' attualmente attiva sui servers e servizi gestiti centralmente dal CIAM e sugli applicativi in SSO

- **Misure strutturali per il backup e la disponibilità dei dati.**

  Sono presenti misure strutturali per il backup per i servers gestiti centralmente dal CIAM e per il PTA viene usato onedrive

- **Gestione completa del ciclo degli account (utenti, amministratori, account tecnici) e delle autorizzazioni (dalla creazione alla chiusura, incluse le sospensioni)**

  Il ciclo di vita degli accounts istituzionali si basa su prassi consolidate anche in rapporto alla relazione dell'utente con l'ente. Alcune classi di utenti tuttavia possono autorizzare account esterni, tramite procedura definita.

  Le autorizzazioni sui servizi e server centrali sono gestiti centralmente, su servizi l'autorizzazione viene di norma gestità dal responsabile di servizio. L'utilizzo di account centrali non è obbligatorio/implementato per tutti i servizi.

  Tuttavia l'accesso alle stazioni di lavoro NON PTA può essere effettuato con utenze locali non gestite centralmente

- **Restrizione e controllo dell'accesso a locali, apparecchiature e dati in base a permessi/funzioni ("need-to-know").**

  L'accesso ai locali ospitanti le sale macchine in gestione al CIAM è regolato da sistema di controllo di accessi, cosi come i dati sono di norma applicati i principi del need-to-know.
  I dipartimenti gestiscono in autonomia accessi fisici, apparecchiature e dati (ad

esclusione degli apparati serventi la rete)

- **Misure di gestione delle vulnerabilità tecniche (rilevamento, patching, ecc.).**

  Vengono effettuati dei VA e PT, il patching sui clients/servers gestiti centralmente (Server centrali e postazioni PTA) è impostato centralmente cosi come il rilevamento. La correzione delle vulnerabilità sui server o client non ha tempistiche certe.

Telecamere di sicurezza all'ingresso dei locali

Sono presenti telecamere di sicurezza all'accesso dei locali ospitanti la sala macchine del CIAM (Centro Informatico Ateneo Messinese)

Misure organizzative

☐ Politica di sicurezza del sistema informativo e politica di protezione dei dati (scenario di violazione dei dati, procedura di arrivo e partenza del personale, best practice ICT, ecc.).
☐ Sensibilizzazione e formazione del personale e dei collaboratori esterni coinvolti nel trattamento dei dati personali.
X Nomina di un responsabile della protezione dei dati o di un responsabile della gestione della protezione dei dati (DPO).
X Nomina di un responsabile della sicurezza informatica.
☐ Organigramma interno e chiara suddivisione dei compiti.
☐ Personale vincolato dal segreto professionale o da un accordo di riservatezza.
X Prevenzione, individuazione e trattamento dei rischi fisici (incendi, danni da acqua, ecc.).
☐ Processo di cancellazione sicura dei dati (ad es. distruggidocumenti, ecc.).
☐ Piano di ripristino, di disastro o di emergenza (piano di continuità operativa e di ripristino).
☐ Procedura di gestione degli incidenti di sicurezza.
☐ Registro degli incidenti in relazione al monitoraggio operativo dell'elaborazione.
☐ Audit periodico dell'ambiente, delle soluzioni e delle procedure.
X Misure di informazione per gli interessati (informativa sulla privacy, politica sui cookie nei siti e/o nelle web-app, ecc.).
X Altro (specificare): **Le seguenti misure organizzative non sono selezionate in quanto non sono applicate globalmente:**

- **Sensibilizzazione e formazione del personale e dei collaboratori esterni coinvolti nel trattamento dei dati personali.**

  Sono stati effettuati dei corsi interni e simulazioni di phishing ad una parte del PTA in merito a cybersecurity e GDPR. Non è stata selezionata in quanto non copre l'intero personale dell'organizzazione.

- **Organigramma interno e chiara suddivisione dei compiti.**

  E' presente un organigramma ma non è presente un funzionigramma aziendale con chiara suddivisione dei compiti

- **Personale vincolato dal segreto professionale o da un accordo di riservatezza**
  Le suddette specificazioni sono inserite nelle autorizzazioni al trattamento ai sensi dell'art. 29 del Regolamento EU n. 679/2016 (GDPR) e ai sensi dell'art. 2-quaterdeciaes del D.çgs 101/2018 (Codice in materia di protezione dei dati personali)

- **Procedura di gestione degli incidenti di sicurezza.**

  Non esiste una procedura formale e standard per la gestione di tutte le tipologie degli incidenti di sicurezza. In esercizio una procedura in relazione ai furti di identità.

- **Registro degli incidenti in relazione al monitoraggio operativo dell'elaborazione**
  Con riferimento alla violazione di dati personali,

Allegato 2 c)

MISURE TECNICHE ED ORGANIZZATIVE IN USO PRESSO UNIVERSITA'DEGLI STUDI DI NAPOLI FEDERICO II

Misure Tecniche

☒ Misure di protezione delle singole apparecchiature informatiche (antivirus, aggiornamenti e patch di sicurezza, test, ecc.).
☒ Misure di protezione fisica dei locali e delle apparecchiature (accesso tramite chiave o codice o badge; elenco aggiornato delle persone autorizzate; registro dei visitatori; videosorveglianza; allarme, ecc.).
☐ Misure di protezione logica per l'accesso alle apparecchiature, ai server e ai dati (accesso con identificatore unico e meccanismo di autenticazione, ecc.).
☒ Misure strutturali per il backup e la disponibilità dei dati.
☐ Misure per la crittografia dei supporti di memorizzazione dei dati.
☐ Misure di crittografia per il trasferimento dei dati.
☒ Misure che assicurano una maggiore pseudonimizzazione delle informazioni in ambienti di test.
 Gestione completa del ciclo degli account (utenti, amministratori, account tecnici) e delle autorizzazioni (dalla creazione alla chiusura, incluse le sospensioni).
☒ Restrizione e controllo dell'accesso a locali, apparecchiature e dati in base a permessi/funzioni ("need-to-know").
☒ Misure di tracciabilità: registrazione dell'accesso dell'utente all'ambiente (tracciamento delle connessioni locali e remote), dati registrati (ad es. login, data e ora della connessione, ecc.) e periodo di conservazione.
☒ Sistema di prevenzione e rilevamento delle intrusioni di rete.
☒ Misure di gestione delle vulnerabilità tecniche (rilevamento, patching, ecc.).
☐ Telecamere di sicurezza all'ingresso dei locali.
☐ Controllo e gestione dei supporti rimovibili per prevenire la divulgazione, la modifica, la cancellazione o la distruzione non autorizzata di dati personali.
☒ Dispositivi di archiviazione sicuri per proteggere i registri e le apparecchiature e prevenire la perdita, il danneggiamento, il furto o la messa in pericolo dei dati personali.
☐ Altro (specificare):

Misure organizzative

☐ Politica di sicurezza del sistema informativo e politica di protezione dei dati (scenario di violazione dei dati, procedura di arrivo e partenza del personale, best practice ICT, ecc.).
☒ Sensibilizzazione e formazione del personale e dei collaboratori esterni coinvolti nel trattamento dei dati personali.
☒ Nomina di un responsabile della protezione dei dati o di un responsabile della gestione della protezione dei dati (DPO).
☒ Nomina di un responsabile della sicurezza informatica.
☒ Organigramma interno e chiara suddivisione dei compiti.
☒ Personale vincolato dal segreto professionale o da un accordo di riservatezza.

☒Prevenzione, individuazione e trattamento dei rischi fisici (incendi, danni da acqua, ecc.).
☒ Processo di cancellazione sicura dei dati (ad es. distruggidocumenti, ecc.).
☒ Piano di ripristino, di disastro o di emergenza (piano di continuità operativa e di ripristino).
☒Procedura di gestione degli incidenti di sicurezza.
☐ Registro degli incidenti in relazione al monitoraggio operativo dell'elaborazione.
☐ Audit periodico dell'ambiente, delle soluzioni e delle procedure.
☒ Misure di informazione per gli interessati (informativa sulla privacy, politica sui cookie nei siti e/o nelle web-app, ecc.).
☐ Altro (specificare):

Allegato 2 d)

MISURE TECNICHE ED ORGANIZZATIVE IN USO PRESSO UNIVERSITA'DEGLI STUDI MAGNA GRAECIA DI CATANZARO

Misure Tecniche

☒ Misure di protezione delle singole apparecchiature informatiche (antivirus, aggiornamenti e patch di sicurezza, test, ecc.).

☒ Misure di protezione fisica dei locali e delle apparecchiature (accesso tramite chiave o codice o badge; elenco aggiornato delle persone autorizzate; registro dei visitatori; videosorveglianza; allarme, ecc.).

☒ Misure di protezione logica per l'accesso alle apparecchiature, ai server e ai dati (accesso con identificatore unico e meccanismo di autenticazione, ecc.).

☒ Misure strutturali per il backup e la disponibilità dei dati.

☐ Misure per la crittografia dei supporti di memorizzazione dei dati.

☒ Misure di crittografia per il trasferimento dei dati.

☐ Misure che assicurano una maggiore pseudonimizzazione delle informazioni in ambienti di test.

☐ Gestione completa del ciclo degli account (utenti, amministratori, account tecnici) e delle autorizzazioni (dalla creazione alla chiusura, incluse le sospensioni).

☒ Restrizione e controllo dell'accesso a locali, apparecchiature e dati in base a permessi/funzioni ("need-to-know").

☐ Misure di tracciabilità: registrazione dell'accesso dell'utente all'ambiente (tracciamento delle connessioni locali e remote), dati registrati (ad es. login, data e ora della connessione, ecc.) e periodo di conservazione.

☐ Sistema di prevenzione e rilevamento delle intrusioni di rete.

☐ Misure di gestione delle vulnerabilità tecniche (rilevamento, patching, ecc.).

☒ Telecamere di sicurezza all'ingresso dei locali.

☐ Controllo e gestione dei supporti rimovibili per prevenire la divulgazione, la modifica, la cancellazione o la distruzione non autorizzata di dati personali.

☐ Dispositivi di archiviazione sicuri per proteggere i registri e le apparecchiature e prevenire la perdita, il danneggiamento, il furto o la messa in pericolo dei dati personali.

☐ Altro (specificare):

Misure organizzative

☐ Politica di sicurezza del sistema informativo e politica di protezione dei dati (scenario di violazione dei dati, procedura di arrivo e partenza del personale, best practice ICT, ecc.).

☐ Sensibilizzazione e formazione del personale e dei collaboratori esterni coinvolti nel trattamento dei dati personali.

☒ Nomina di un responsabile della protezione dei dati o di un responsabile della gestione della protezione dei dati (DPO).

☐ Nomina di un responsabile della sicurezza informatica.

☒ Organigramma interno e chiara suddivisione dei compiti.

☐ Personale vincolato dal segreto professionale o da un accordo di riservatezza.

- ☒ Prevenzione, individuazione e trattamento dei rischi fisici (incendi, danni da acqua, ecc.)
- ☒ Processo di cancellazione sicura dei dati (ad es. distruggidocumenti, ecc.).
- ☐ Piano di ripristino, di disastro o di emergenza (piano di continuità operativa e di ripristino).
- ☐ Procedura di gestione degli incidenti di sicurezza.
- ☐ Registro degli incidenti in relazione al monitoraggio operativo dell'elaborazione.
- ☒ Audit periodico dell'ambiente, delle soluzioni e delle procedure.
- ☒ Misure di informazione per gli interessati (informativa sulla privacy, politica sui cookie nei siti e/o nelle web-app, ecc.).
- ☐ Altro (specificare):