Egregio Prof. <NOME COGNOME DOCENTE>

Dipartimento di <NOME DIPARTIMENTO>

Università degli Studi di Parma

\_\_\_\_\_\_\_\_\_\_\_\_\_

**ATTO DI DESIGNAZIONE A**

**DELEGATO AL TRATTAMENTO DEI DATI**

**nell’ambito dello Studio “<NOME STUDIO>”**

**Titolo dello Studio**: “TITOLO DESCRITTIVO STUDIO” di seguito solo lo “Studio”.

**Università degli Studi di Parma (di seguito “Università “o il “Titolare”),** con sede in Via Gramsci 14 – Parma, nella persona del legale rappresentante, Titolare del trattamento dei dati personali,

**DESIGNA**

**DELEGATO AL TRATTAMENTO DEI DATI PERSONALI**

ai sensi degli artt. 29 e 32, par. 4, del Regolamento (UE) 2016/679 e 2-quaterdecies del D. Lgs. 30 giugno 2003, n. 196, e del Regolamento di Ateneo DR N. 346/2023

**il Prof.** <NOME COGNOME DOCENTE>

in qualità di PI (Principal Investigator – Responsabile della ricerca), **nell’ambito dello Studio sopra riportato,** effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l’ambito di funzioni e competenze attribuite.

Il Delegato risulta essere stato individuato per esperienza, capacità ed affidabilità tali da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza, ed ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in esse previsto, nonché osservare le istruzioni impartite dal Titolare.

**Istruzioni operative per il trattamento dei dati da parte del DELEGATO**

Nello svolgimento della delega attribuita la S.V. dovrà attenersi alle seguenti disposizioni:

* **trattare** i dati personali solo su istruzione del Titolare del trattamento e garantire la corretta applicazione del Regolamento generale per la protezione dei dati (GDPR) e del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, nonché la conformità alle indicazioni dell’Autorità Garante per la protezione dei dati personali;
* **designare** i propri collaboratori quali Autorizzati al trattamento dei dati personali per i trattamenti di dati di propria competenza, in modalità scritta (modulo ISTRUZIONI FUNZIONALI AL TRATTAMENTO DI DATI PERSONALI – STUDIO < **NOME STUDIO>**) e secondo livelli differenziati, conservando il relativo atto;
* **fornire** agli Autorizzati istruzioni conformi alle disposizioni aziendali circa le corrette modalità da seguire e le misure di sicurezza da adottare per il trattamento dei dati personali, e richiedendo, se del caso, il rilascio delle credenziali per l’accesso ai software di competenza utilizzando la modulistica in uso;
* **verificare** periodicamente che i dati personali oggetto di trattamento nello specifico ambito di competenza siano esatti, aggiornati, pertinenti e non eccedenti e che questi siano conservati in una

forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;

* **osservare** e fare osservare ai designati Autorizzati:
1. Regolamento di Ateneo “Regolamento di sicurezza delle informazioni e utilizzo delle risorse informatiche”, DR N. 390/2022
2. Regolamento di Ateneo “REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI”, DR N. 346/2023, in particolare, art. 9 – Autorizzati al trattamento, art. 10 – I Designati al trattamento, art. 10.3 – I Responsabili scientifici, art. 12 – Sensibilizzazione e formazione, art. 21 – Comunicazione e diffusione dei dati relativi ad attività di studio e ricerca, art. 26 – Trattamenti dai fini di ricerca medica ed epidemiologica, art. 27 – Sicurezza, art. 30 – Violazione di dati personali (Databreach)
3. le istruzioni di carattere generale impartire dal Titolare a tutti i soggetti autorizzati al trattamento (es. Istruzioni operative sul corretto trattamento dei dati rivolte a tutti i dipendenti/collaboratori);
4. eventuali ulteriori specifiche istruzioni predisposte dallo stesso Delegato in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.
* **verificare** che i dati oggetto di trattamento siano esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;
* **attenersi** alle indicazioni di sicurezza dettate dal Titolare del trattamento e compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;
* **partecipare** ai momenti formativi organizzati dal Titolare ed assicurare la partecipazione dei propri autorizzati;
* **collaborare** con i competenti servizi per la compilazione e l’aggiornamento del Registro dei trattamenti del Titolare;
* **non** porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
* **segnalare** senza ritardo al Titolare del trattamento, ogni violazione di dati personali (c.d. Data Breach) di cui si abbia conoscenza nell’ambito delle attività di ricerca e collaborare alla istruttoria del caso al fine di sottoporre al DPO ogni utile e opportuna determinazione in merito.
* **Vigilare che gli Autorizzati:**
	+ **trattino** i dati personali, qualora necessari e pertinenti, nel rispetto dei principi di liceità, correttezza e trasparenza, e con specifici accorgimenti e modalità tali da garantire la tutela della dignità e delle libertà individuali dell’interessato e la confidenzialità nelle comunicazioni;
	+ **rispettino** il segreto d’ufficio e il segreto professionale o altri obblighi equivalenti di segretezza;
	+ **rispettino** le adeguate misure di sicurezza organizzative e tecniche impartite dall’Università e dal Delegato per proteggere i dati personali;
	+ **non comunichino** e/o diffondano i dati personali, neppure ricorrendo a sistemi di comunicazione digitale (tipo social network o messaggistica), a soggetti non autorizzati, e non li utilizzino per fini personali, anche attraverso la loro acquisizione tramite dispositivi personali, come ad esempio telefono cellulare, memoria USB, pc, ecc...;
	+ **utilizzino** la documentazione cartacea, nonché i supporti rimovibili su cui sono memorizzati i dati personali (qualora autorizzati), osservando le istruzioni operative impartite dal Titolare custodendoli con modalità tali da evitare accessi non autorizzati e trattamenti non consentiti dei dati.
	+ **provvedano** a distruggere ogni eventuale copia della documentazione o dei dati personali acquisiti per lo Studio.

La S.V. dovrà altresì **verificare** che:

* + siano impiegate specifiche misure e accorgimenti tecnici per incrementare il livello di sicurezza dei dati trattati per l’esecuzione dello Studio, sia nella fase di memorizzazione o archiviazione, sia nella fase successiva di elaborazione delle informazioni, nonché nella successiva fase di trasmissione dei dati, individuando la categoria dei dati personali trattati: ovvero se trattasi di dati comuni o particolari (es: relativi alla salute), in modo da assegnare un adeguato livello di sicurezza (pseudonimizzazione, tecniche di cifratura, …).
	+ siano adottati, in particolare:
1. gli accorgimenti adeguati a garantire la qualità dei dati e la corretta attribuzione agli interessati;
2. gli idonei accorgimenti per garantire la protezione dei dati dello Studio dai rischi di accesso abusivo ai dati, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l’applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l’adozione di altre misure che rendano inintelligibili i dati ai soggetti non legittimati) nelle operazioni di registrazione e archiviazione dei dati;
3. i canali di trasmissione protetti, tenendo conto dello stato dell’arte della tecnologia, nei casi in cui si renda necessaria la comunicazione dei dati raccolti nell’ambito dello Studio a una banca dati centralizzata dove sono memorizzati e archiviati oppure ad un promotore o a soggetti esterni di cui lo stesso promotore si avvale per la conduzione dello Studio.
4. le tecniche di etichettatura, nella conservazione e nella trasmissione di campioni biologici, mediante codici identificativi, oppure altre soluzioni che, considerato il numero di campioni utilizzati, li rendono non direttamente riconducibili agli interessati, permettendo di identificare questi ultimi solo in caso di necessità;
5. con specifico riferimento alle operazioni di elaborazione dei dati dello Studio memorizzati in una banca dati centralizzata, è necessario adottare:
	* idonei sistemi di autenticazione e di autorizzazione per il personale preposto al trattamento in funzione dei ruoli e delle esigenze di accesso e trattamento, avendo cura di utilizzare credenziali di validità limitata alla durata dello Studio e di disattivarle al termine dello stesso;
	* procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti designati al trattamento;
	* sistemi di controllo degli accessi al database e per il rilevamento di eventuali anomalie.

In ordine al **salvataggio** dei dati, il Delegato dovrà:

* valutare con il supporto tecnico, il tipo di supporto/dispositivo su cui salvare i dati personali trattati e che siano attive politiche adeguate di backup dei dati sia nel caso in cui gli stessi vengano memorizzati su sistemi di storage dell’Università, che siano salvati sui sistemi del gruppo di ricerca;
* assicurarsi che i dati personali non vengano salvati dai collaboratori su unità di memoria esterne (hard disk, chiavette, DVD) a meno che non siano autorizzati e dotati di appositi sistemi di cifratura (in modo da proteggere i dati anche nel caso in cui tali unità di memoria vengano smarrite o rubate);
* verificare con il supporto tecnico la completa cancellazione dei dati in caso di dismissione/riparazione/riutilizzo di hardware o dispositivi contenente i dati stessi.

In ordine alle procedure di Autenticazione e Autorizzazione il Delegato dovrà:

* individuare i soggetti autorizzati a trattare i dati personali, definendo con il supporto tecnico le corrette autorizzazioni di accesso ai dispositivi e alle aree ove i dati sono trattati/conservati; qualora non sussistano più le ragioni per l’accesso ai dati (ad es. uscita di un ricercatore dal team di ricerca, conclusione del progetto di ricerca) procedere a far rimuovere tempestivamente le relative autorizzazioni;
* adottare meccanismi di autenticazione (pin, password) per l’accesso al dato e/o ai sistemi che trattano il dato, attivando meccanismi di crittografia dei supporti fisici per tutti i sistemi.

La presente designazione, che potrà essere oggetto di revisione, ha efficacia per la sola durata dello Studio e fino ad una successiva ed ulteriore delega o fino alla risoluzione del rapporto di lavoro o collaborazione per qualsiasi causa oppure fino alla revoca da parte del Titolare.

**Luogo e data, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Il Titolare del trattamento dei dati personali**

**Università di Parma**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Il Delegato per presa visione e accettazione**

**Prof.** <NOME COGNOME DOCENTE>

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**