IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

DELIBERAZIONE N. **355** DEL **22/04/2024**

OGGETTO: PRESA D'ATTO STIPULA ATTI DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI EX ARTT. 28-29 REGOLAMENTO EUROPEO 27 APRILE 2016, N.679-GDPR NEI CONFRONTI DEL CONSORZIO DI BIOINGEGNERIA E INFORMATICA MEDICA – CBIM, DA PARTE DI IRCCS ISTITUTI FISIOTERAPICI OSPITALIERI-IFO, ISTITUTO NAZIONALE TUMORI REGINA ELENA (IRE) E ISTITUTO DERMATOLOGICO SANTA MARIA E SAN GALLICANO (ISG), TITOLARI DEL TRATTAMENTO DEI DATI

Esercizi/o e conto / Centri/o di costo / **- Importo presente Atto: € /** **- Importo esercizio corrente: € /** Budget **- Assegnato: € -** **- Utilizzato: € -** **- Residuo: € -** **Autorizzazione n°: -** Servizio Risorse Economiche: **Francesca Romana Benedetto**	STRUTTURA PROPONENTE **UOSD Servizio Amministrativo Ricerca** Il Dirigente Responsabile **Ottavio Latini** Responsabile del Procedimento **Chiara Giuliani** L'Estensore **Chiara Giuliani** Proposta n° DL-363-2024
PARERE DEL DIRETTORE SANITARIO Positivo Data 22/04/2024 IL DIRETTORE SANITARIO **Ermete Gallo**	**PARERE DEL DIRETTORE AMMINISTRATIVO** Positivo Data 22/04/2024 IL DIRETTORE AMMINISTRATIVO **Laura Figorilli**

Parere del Direttore Scientifico IRE **Gennaro Ciliberto** data 19/04/2024 Positivo

Parere del Direttore Scientifico ISG ad interim **Gennaro Ciliberto** data 19/04/2024 Positivo

La presente deliberazione si compone di n° 7 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:
All. 1
All. 2

Il Dirigente della UOSD Servizio Amministrativo Ricerca

Visto il decreto legislativo del 30 dicembre 1992, n. 502 e successive modificazioni ed integrazioni;

Visto il decreto legislativo 16 ottobre 2003, n. 288 e il decreto legislativo 23 dicembre 2022, n. 200 "Riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico";

Vista la legge regionale 23 gennaio 2006, n. 2;

Visto l'Atto Aziendale adottato con deliberazione n. 153 del 19 febbraio 2019 e approvato dalla Regione Lazio con DCA n. U00248 del 2 luglio 2019, modificato e integrato con deliberazioni n. 1254 del 02 dicembre 2020, n. 46 del 2 gennaio 2021 e n. 380 del 25 marzo 2021, approvate dalla Direzione Salute e Integrazione Sociosanitaria della Regione Lazio, con Determinazione n. G03488 del 30 marzo 2021;

Vista la deliberazione IFO n. 1 del 2 gennaio 2024 di insediamento del Direttore Generale f.f. Dott.ssa Laura Figorilli;

Viste le deliberazioni n. 212 del 16 marzo 2022 e n. 154 del 28 febbraio 2022 con le quali sono stati nominati rispettivamente la Dott.ssa Laura Figorilli quale Direttore Amministrativo ed il Dott. Ermete Gallo quale Direttore Sanitario degli Istituti Fisioterapici Ospitalieri;

Visto il D.M. del Ministero della Salute del 8 maggio 2020 di conferma del riconoscimento del carattere scientifico dell'IRCCS di diritto pubblico a Istituti Fisioterapici Ospitalieri (IFO) relativamente alla disciplina di "oncologia" per l'Istituto Nazionale Tumori Regina Elena (IRE) e alla disciplina di "dermatologia" per l'Istituto San Gallicano (ISG);

Premesso che gli artt. 8 e 9 del suddetto decreto, come da ultimo modificati dal D.lgs. 23 dicembre 2022, n. 200, prevedono la possibilità per gli IRCCS di stipulare accordi e convenzioni, costituire e/o partecipare a consorzi e attuare misure di collegamento e sinergia con altre strutture di ricerca e assistenza sanitaria, pubbliche e private, nonché con le Università, per la realizzazione di comuni progetti di ricerca, in conformità all'art. 15 L. n. 241/1990;

che l'art. 10 del decreto legislativo 16 ottobre 2003 n. 288, contempla le diverse tipologie di ricavi degli IRCCS;

che, in esecuzione alla determina n. 206 del 19 marzo 2024, sono state autorizzate le liquidazioni delle fatture n. 56 per gli IRCCS Istituti Fisioterapici Ospitalieri-IFO, Istituto Nazionale Tumori Regina Elena (di seguito "IFO-IRE") e n. 57 per gli IRCCS Istituti Fisioterapici Ospitalieri-IFO, Istituto Dermatologico Santa Maria e San Gallicano (di seguito "IFO-ISG") del 29 febbraio 2024 relative all'adesione al Consorzio di Bioingegneria e Informatica Medica - CBIM da parte dei due Istituti, comprensiva di servizi di base informatici;

che, in esecuzione alla deliberazione n. 267 del 28 marzo 2024, si è proceduto all'adesione di IFO-IRE al Consorzio di Bioingegneria e Informatica Medica – CBIM;

che, in esecuzione alla deliberazione n. 268 del 28 marzo 2024, si è proceduto all'adesione di IFO-ISG al Consorzio di Bioingegneria e Informatica Medica – CBIM;

che il Consorzio di Bioingegneria e Informatica Medica – CBIM svolge per IFO-IRE e IFO-ISG servizi informatici di base/consulenza per il caricamento dati sul Workflow della Ricerca del Ministero della Salute;

che tali servizi informatici comportano il trattamento di dati personali di cui IFO-IRE e IFO-ISG, "Enti Partecipanti" al Consorzio, si qualificano, ai fini del Regolamento europeo 27 aprile 2016, n.679 – GDPR, come Titolari del trattamento dei dati ex art. 4, paragrafo 7;

che, conseguentemente, il Consorzio di Bioingegneria e Informatica Medica – CBIM si qualifica ex artt. 28-29 GDPR come Responsabile del trattamento dei dati e, pertanto, è stato formalmente nominato con atti di nomina, rispettivamente di IFO-IRE e di IFO-ISG, sottoscritti in data 10 aprile 2024, che, allegati al presente atto, ne costituiscono parte integrante e sostanziale (All. 1 e All. 2);

Ritenuto opportuno prendere atto della sottoscrizione tra le Parti, avvenuta in data 10 aprile 2024, dell'atto di nomina a Responsabile del trattamento dei dati ex artt. 28-29 Regolamento europeo 27 aprile 2016, n.679 - GDPR nei confronti del Consorzio di Bioingegneria e Informatica Medica – CBIM, da parte di IRCCS Istituti Fisioterapici Ospitalieri-IFO, Istituto Nazionale Tumori Regina Elena, Titolare del trattamento, che, allegato al presente atto, ne costituisce parte integrante e sostanziale (All. 1);

opportuno prendere atto della sottoscrizione tra le Parti, avvenuta in data 10 aprile 2024, dell'atto di nomina a Responsabile del trattamento dei dati ex artt. 28-29 Regolamento europeo 27 aprile 2016, n.679 - GDPR nei confronti del Consorzio di Bioingegneria e Informatica Medica – CBIM, da parte di IRCCS Istituti Fisioterapici Ospitalieri-IFO, Istituto Dermatologico Santa Maria e San Gallicano, Titolare del trattamento, che, allegato al presente atto, ne costituisce parte integrante e sostanziale (All. 2);

Attestato che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e successive modifiche, nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005.

Propone

Per i motivi di cui in narrativa che si intendono integralmente confermati di:

- prendere atto della sottoscrizione tra le Parti, avvenuta in data 10 aprile 2024, dell'atto di nomina a Responsabile del trattamento dei dati ex artt. 28-29 Regolamento europeo 27 aprile 2016, n.679 - GDPR nei confronti del Consorzio di Bioingegneria e Informatica Medica – CBIM, da parte di IRCCS Istituti Fisioterapici Ospitalieri-IFO, Istituto Nazionale Tumori Regina Elena, Titolare del trattamento, che, allegato al presente atto, ne costituisce parte integrante e sostanziale (All. 1);

- prendere atto della sottoscrizione tra le Parti, avvenuta in data 10 aprile 2024, dell'atto di nomina a Responsabile del trattamento dei dati ex artt. 28-29 Regolamento europeo 27 aprile 2016, n.679 - GDPR nei confronti del Consorzio di Bioingegneria e Informatica Medica – CBIM, da parte di IRCCS Istituti Fisioterapici Ospitalieri-IFO, Istituto Dermatologico Santa Maria e San Gallicano, Titolare del trattamento, che, allegato al presente atto, ne costituisce parte integrante e sostanziale (All. 2).

La UOSD Servizio Amministrativo per la Ricerca curerà tutti gli adempimenti per l'esecuzione della presente deliberazione.

Il Dirigente della UOSD Servizio Amministrativo Ricerca

Ottavio Latini

Il Direttore Generale f.f.

Visto il decreto legislativo 30 dicembre 1992, n. 502 e s.m.i.;

Vista la legge regionale 23 gennaio 2006, n. 2;

Visto l'Atto Aziendale adottato con deliberazione n. 153 del 19 febbraio 2019 ed approvato dalla Regione Lazio con DCA n. U00248 del 2 luglio 2019, modificato e integrato con deliberazioni n. 1254 del 02 dicembre 2020, n. 46 del 21 gennaio 2021 e n. 380 del 25 marzo 2021, approvate dalla Direzione Salute e Integrazione Socio-sanitaria della Regione Lazio, con Determinazione n. G03488 del 30 marzo 2021;

Visto l'art. 3 comma 6 del D.lgs. 502/92 e successive modificazioni ed integrazioni, non ché l'art. 8 comma 7 della L.R. del Lazio n. 18/94.

Vista la deliberazione IFO n. 1 del 2 gennaio 2024 di insediamento del Direttore Generale f.f. Dott.ssa Laura Figorilli;

Preso atto che il Dirigente proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e s.m.i., nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005.

Visto il parere favorevole del Direttore Amministrativo e del Direttore Sanitario Aziendale;

ritenuto di dover procedere;

Delibera

di approvare la proposta così formulata concernente *"PRESA D'ATTO STIPULA ATTI DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI EX ARTT. 28-29 REGOLAMENTO EUROPEO 27 APRILE 2016, N.679-GDPR NEI CONFRONTI DEL CONSORZIO DI BIOINGEGNERIA E INFORMATICA MEDICA – CBIM, DA PARTE DI IRCCS ISTITUTI FISIOTERAPICI OSPITALIERI-IFO, ISTITUTO NAZIONALE TUMORI REGINA ELENA (IRE) E ISTITUTO DERMATOLOGICO SANTA MARIA E SAN GALLICANO (ISG), TITOLARI DEL TRATTAMENTO DEI DATI"* e di renderla disposta.

Il Direttore Generale f.f.

Dr.ssa Laura Figorilli

Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

CONTRATTO DI INDIVIDUAZIONE DEL RESPONSABILE DEL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N.679

Gli IRCCS Istituti Fisioterapici Ospitalieri IFO – Istituto Nazionale Tumori Regina Elena IRE, con sede legale in Via Elio Chianesi, 53 – 00144 Roma, Codice Fiscale 02153140583, Partita Iva 01033011006, nella persona del legale rappresentante *f.f.* Dott.ssa Laura Figorilli, di seguito indicata come DATA CONTROLLER/TITOLARE

e

CBIM – Consorzio di Bioingegneria e Informatica Medica (in seguito "CBIM"), con sede legale in Piazzale Volontari del Sangue n. 2 – 27100 Pavia (IT) - P.IVA 01515320180, nella persona del legale rappresentante pro-tempore, di seguito DATA PROCESSOR/RESPONSABILE

Di seguito, quando indicate congiuntamente, le "Parti"

PREMESSO CHE

a) Il 4 maggio 2016 è stato pubblicato in Gazzetta Ufficiale Europea il Regolamento generale per la protezione dei dati personali – Regolamento UE 2016-679 (anche GDPR);
b) Il Regolamento UE 2016/679 è entrato in vigore il 24 maggio 2016 ed è effettivamente applicabile a partire dal 25 maggio 2018;
c) Il 19 settembre 2018 è entrato in vigore il D.lgs. 101/2018 che ha introdotto le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679;
d) L'art. 28 GDPR prevede che il Titolare del trattamento, individuato ai sensi dell'art. 4 n. 7 GDPR, possa avvalersi di uno o più Responsabili del trattamento dei dati che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di tale Regolamento e garantisca la tutela dei diritti dell'interessato;
e) Il Titolare è stato ammesso quale Ente Partecipante a CBIM e nell'ambito di tale rapporto CBIM svolge per esso il servizio di consulenza per il caricamento dati sul Workflow della Ricerca del Ministero della Salute, come da documentazione richiamata nella richiesta di adesione quale Ente Partecipante a suo tempo trasmessa a CBIM, alla quale si fa integrale rinvio*;*
f) Tale servizio affidato a CBIM comporta il trattamento di dati personali di cui gli IRCCS Istituti Fisioterapici Ospitalieri IFO – Istituto Nazionale Tumori Regina Elena IRE è Titolare;
g) All'interno della **sezione A** del presente documento, oltre all'indicazione del DPO/RPD designato dal responsabile, sono descritte, in relazione all'attività svolta dal responsabile per conto del titolare: le categorie di trattamento, il tipo di dati personali, le categorie di interessati, l'eventuale trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali e le garanzie adottate, gli eventuali sub-responsabili ed il servizio a questi affidato;
h) All'interno della **Sezione B** del presente documento, sono indicati gli obblighi specifici del responsabile in relazione al trattamento effettuato per conto del titolare del trattamento;
i) All'interno della **Sezione C** del presente documento, sono indicate le misure di sicurezza che il responsabile è tenuto a mettere in atto per garantire un livello di sicurezza adeguato al rischio del trattamento dati effettuato per conto del titolare del trattamento;
j) Ai sensi dell'art. 4 GDPR, per trattamento si intende *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l' adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*;
k) alla luce delle verifiche documentali effettuate, CBIM possiede l'esperienza, la capacità, l'affidabilità e fornisce idonee garanzie del pieno rispetto delle disposizioni vigenti in materia di trattamento dati, ivi compreso il profilo della sicurezza in relazione alle finalità e alle

modalità delle operazioni di trattamento nonché alle garanzie di tutela dei diritti dell'interessato;

l) le parti intendono regolare, con il presente atto, i loro reciproci rapporti in tema di disciplina del trattamento dei dati personali.

Tutto ciò premesso, che costituisce parte integrante del presente atto, DATA CONTROLLER individua ai sensi dell'art. 28 GDPR

CBIM – Consorzio di Bioingegneria e Informatica Medica (in seguito "CBIM"), con sede legale in Piazzale Volontari del Sangue n. 2 – 27100 Pavia (IT) - P.IVA 01515320180

quale Responsabile del trattamento dei dati personali in relazione al trattamento dei dati personali effettuato in forza del contratto sopracitato.

CONTRATTO DI NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

1. OGGETTO E MATERIA

1.1. Con la stipula del presente atto, ai sensi dell'articolo 28 GDPR, il titolare designa CBIM "responsabile" delle operazioni di trattamento dei dati personali affidati. In virtù di tale nomina e del rapporto associativo intercorrente tra le Parti, il responsabile è autorizzato al trattamento dei dati per conto del titolare, così come descritto nel presente documento e nelle sezioni che lo compongono.

1.2. Il contenuto del presente atto, in quanto compatibile, si applica anche ai trattamenti effettuati dagli IRCCS Istituti Fisioterapici Ospitalieri IFO – Istituto Nazionale Tumori Regina Elena IRE quale responsabile per conto di un titolare terzo rispetto al cui trattamento CBIM si configura quale sub-responsabile. Le parti si riservano di integrare ovvero sostituire il presente atto qualora necessario.

2. OBBLIGHI DEL RESPONSABILE

2.1. La sottoscrizione del presente atto vincola il responsabile del trattamento al titolare del trattamento e fa sorgere in capo al responsabile una serie di obblighi specificamente individuati nella **Sezione B** del presente documento.

3. MISURE DI SICUREZZA E VIOLAZIONE DEI DATI

3.1. Il responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR). Si veda la **Sezione C** del presente documento.

4. DECORRENZA, DURATA, CESSAZIONE DEL TRATTAMENTO

4.1. Il ruolo e le competenze assegnate al responsabile del trattamento con il presente atto hanno la medesima durata ed efficacia della partecipazione, quale Ente Partecipante, del Titolare a CBIM e pertanto si intendono tacitamente rinnovate ogni anno fino alla cessazione della qualifica stessa o fino alla revoca da parte del titolare.

4.2. Dopo il completamento del trattamento per conto del titolare, il responsabile deve, su istruzione del titolare del trattamento, restituire o cancellare i dati personali e le relative copie esistenti, salvo che non siano previste specifiche e differenti politiche di conservazione dei dati (anche in relazione alle categorie di dati trattati) a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento.

4.2.1. Il responsabile deve rilasciare contestualmente un'attestazione scritta che presso lo stesso non esiste alcuna copia dei dati personali trattati in nome e per conto del titolare del trattamento.

5. COMUNICAZIONI TRA LE PARTI

5.1. Le comunicazioni tra le parti, ai fini del presente incarico, dovranno avvenire:

-per il titolare, a dirscire@ifo.it

- per il responsabile, a amministrazione@cbim.it

6. DISPOSIZIONI VARIE

6.1. Il corrispettivo per il presente incarico di responsabile del trattamento rimane ad ogni effetto ricompreso nella quota annuale associativa versata dal Titolare a CBIM in quanto Ente Partecipante.

6.2. Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

6.3. I termini utilizzati all'interno del presente atto hanno lo stesso significato dalla GDPR e dal D. Lgs. 196/2003.
6.3.1. Il presente atto deve essere letto e interpretato secondo quanto disposto dalla GDPR e dal D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018).
6.4. Con l'occasione, il titolare ricorda l'importanza delle prescrizioni di legge in materia di trattamento dei dati personali, nonché il fatto che la violazione di dette normative può comportare responsabilità sia civili che penali per il titolare e per il responsabile, con possibile applicazione di sanzioni amministrative e pecuniarie, ai sensi degli artt. 82, 83 e 84 GDPR.
6.5. Il presente contratto sostituisce qualsiasi altro accordo, contratto o intesa tra le Parti con riferimento al suo oggetto nonché qualsiasi altra istruzione fornita in precedenza, in qualsiasi altra forma, dal titolare al responsabile. Pertanto, in caso di conflitto tra le disposizioni del presente atto e quelle contenute nel Contratto, prevalgono le disposizioni del presente atto.
6.6. Alla cessazione del rapporto associativo per qualsiasi causa, continueranno ad avere efficacia quelle clausole che per loro natura sopravvivono all'estinzione del rapporto giuridico.
6.7. Il Titolare si riserva il diritto di apportare, in qualsiasi momento, tutte le modifiche ed integrazioni al presente atto d'incarico funzionali al miglior rispetto delle disposizioni della Normativa sulla protezione dei dati personali ovvero delle indicazioni o dei provvedimenti del Garante per la protezione dei dati personali o della magistratura ordinaria.
6.7.1. Le variazioni al presente atto d'incarico, intervenute a norma del precedente punto, saranno efficaci per le Parti dopo che la copia aggiornata dello stesso atto sarà stata sottoscritta da entrambe.
6.8. Il titolare dichiara fin da adesso che i dati personali trasmessi al responsabile sono stati raccolti e trattati legittimamente, sono pertinenti e non eccedenti rispetto alle finalità per cui sono stati raccolti e successivamente trattati, che gli interessati sono stati informati di tale trasmissione e che sussiste un'idonea base giuridica che consente al responsabile di effettuare il trattamento dei dati oggetto del presente contratto di nomina.
6.9. Il presente atto di nomina è soggetto alla legge italiana.
6.9.1. Per qualsiasi controversia riguardante la sua applicazione e/o interpretazione è competente in via esclusiva il Foro di Pavia.

SEZIONE A
TRATTAMENTO EFFETTUATO DAL RESPONSABILE PER CONTO DEL TITOLARE

DATI DI CONTATTO DEL RESPONSABILE PROTEZIONE DEI DATI (RPD/DPO) DEL RESPONSABILE DEL TRATTAMENTO (se nominato): dpo.sicurdata@opendata.it; 055750808

Categorie di trattamento	Tipo di dati personali	Categorie di interessati	Trasferimento verso Paesi terzi o organizzazioni internazionali e garanzie adottate	Sub-responsabili e servizi affidati
Trattamenti necessari all'erogazione dell'attività di caricamento dati sul sistema Workflow della Ricerca	Anagrafici, contrattuali, stipendiali	Ricercatori	Non previsto	Consulenti per attività sistemistica e consulenza applicativa

DATI DI CONTATTO DEL RESPONSABILE PROTEZIONE DEI DATI (RPD/DPO) DEL TITOLARE DEL TRATTAMENTO (se nominato): Scudo Privacy S.r.l., nella persona del Dott. Carlo Villanacci, e-mail: dpo@scudoprivacysrl.com

SEZIONE B
OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO DESIGNATO

In virtù dell'atto che vincola il responsabile designato al Titolare del trattamento, sorgono in capo al responsabile una serie di obblighi.

1. Rispetto delle istruzioni impartite dal titolare

1.1. Il responsabile deve assistere e coadiuvare il titolare nella corretta gestione delle operazioni di trattamento che dovranno essere effettuate nel pieno rispetto degli obblighi previsti dal GDPR e dal D. lgs.196/2003 così come modificato dal D. lgs. 101/2018.

1.2. A tale proposito, il responsabile deve trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un Paese terzo o un'Organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile deve informare il titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

2. Riservatezza

2.1. Il responsabile deve assicurare per sé stesso e per le persone che operano presso la propria azienda, da lui o dal titolare del trattamento autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate.

2.2. Sarà cura del responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il responsabile, in relazione alle operazioni di trattamento da essi eseguite.

3. Conformità a leggi e regolamenti applicabili

3.1. Il responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e del D. lgs. 196/2003 così come modificato dal D. lgs. 101/2018 e, più in generale, ad ogni altra disposizione normativa, nazionale e sovranazionale, in materia di trattamento dei dati personali attualmente in vigore o che in futuro vengano a modificare, integrare o sostituire l'attuale disciplina, nonché ai provvedimenti dell'Autorità Garante competente e alle linee guida adottate dall'*European Data Protection Board*.

4. Misure di sicurezza

4.1. Il responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR).

4.1.1. A tal proposito, si veda la Sezione C del presente documento.

5. Audit

5.1. Il titolare ha diritto di effettuare audit indipendenti per verificare la conformità del responsabile agli obblighi previsti nel presente contratto ed agli adempimenti in materia di protezione dei dati personali.

5.1.1. In tal caso il titolare dovrà previamente inviare richiesta scritta al responsabile e le Parti concorderanno, almeno dieci giorni prima di quando verrà effettuata la verifica, l'oggetto dei controlli e le relative modalità.

5.2. Titolare e responsabile stabiliranno i vincoli di riservatezza a cui devono essere vincolate le Parti e, eventualmente, coloro che effettueranno le verifiche per conto delle Parti stesse.

5.3. Il responsabile deve contribuire alle attività di revisione, comprese le ispezioni, e ad informare prontamente il titolare del trattamento di ogni questione rilevante ai fini del presente contratto quali, a titolo indicativo: istanze degli interessati, richieste del Garante, esiti delle ispezioni, violazioni del GDPR o di altre disposizioni relative alla protezione dei dati.

5.4. Resta inteso che il Titolare avrà la facoltà di incaricare dei professionisti indipendenti per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report ("Report").

5.4.1. Tali Report, che costituiscono informazioni confidenziali, dovranno essere resi disponibili al Responsabile/Subresponsabile per consentirgli di verificare le eventuali azioni correttive da implementare in funzione al presente Atto.
5.4.2. Il Responsabile potrà opporsi per iscritto alla nomina da parte del Titolare di eventuali revisori esterni che siano concorrenti del Responsabile.
5.4.2.1. In tali circostanze, il Titolare sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.
5.4.2.2. Restano a carico esclusivo del Titolare i costi delle attività di verifica dallo stesso commissionate a terzi.

6. Persone autorizzate al trattamento

6.1. Il responsabile, ai sensi dell'art. 29 GDPR e dell'art. 2 *quaterdecies* D. Lgs. 196/2003, si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, alle quali fornisce specifiche istruzioni scritte (salvo che il diritto dell'Unione o degli Stati membri non richieda diversamente, art. 29 GDPR).
6.2. È compito del responsabile designato vigilare sulla corretta esecuzione delle istruzioni impartite.

7. Sub-responsabile

7.1. Il titolare del trattamento autorizza il responsabile del trattamento a ricorrere ai cd. "sub-responsabili" del trattamento indicati nella sezione A per l'esecuzione delle attività di trattamento ivi descritte.
7.2. Il responsabile inoltra al titolare, qualora questo ne faccia richiesta, l'atto di nomina dei sub-responsabili.
7.3. Il responsabile deve informare il titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili, alle quali il titolare del trattamento conserva il diritto di opporsi.
7.4. Al "sub-responsabile" sono imposti, con specifico atto sottoscritto, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto che lega il titolare e il responsabile del trattamento. Il sub-responsabile è tenuto a: osservare, valutare e organizzare la gestione del trattamento dei dati personali e la loro protezione affinché questi siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "*non gli è in alcun modo imputabile*" *(*artt. 82. 1 e 82. 3 GDPR).
7.5. Qualora il sub-responsabile abbia necessità di ricorrere ad ulteriori sub-responsabili, lo comunicherà al responsabile che, a sua volta, inoltrerà tale comunicazione al titolare. Il titolare conserva il diritto di opporsi a tali aggiunte.

8. Registro dei Trattamenti

8.1. Il responsabile deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del titolare del trattamento (art. 30 GDPR).
8.2. Il registro, anche in formato elettronico, deve contenere tutta le informazioni descritte dall'art. 30.2 GDPR.
8.3. Il responsabile del trattamento deve mettere il registro a disposizione dell'Autorità di controllo, se questa ne fa richiesta, affinché possa fungere da strumento per il monitoraggio dei trattamenti effettuati.

9. Esercizio dei diritti dell'interessato

9.1. Il responsabile dovrà informare, tempestivamente e per iscritto, il titolare del trattamento della ricezione di eventuali richieste degli interessati, avanzate ai sensi degli artt. da 15 a 22 del GDPR, ovvero al fine di revocare il consenso prestato e/o proporre reclamo al Garante per la protezione dei dati personali.

10. Valutazione d'impatto sulla protezione dei dati

10.1. Il responsabile del trattamento, se necessario e su richiesta del titolare, dovrà fornire a questi le informazioni necessarie per consentirgli di effettuare la valutazione di impatto ai sensi dell'art. 35 GDPR.

11. Trasferimento dei dati personali all'estero.

11.1. Al Responsabile è fatto divieto di trasferire i dati personali trattati per conto del titolare a Paesi Extra-UE in assenza di un'autorizzazione da parte del titolare e in assenza di: una decisione di adeguatezza (art. 45 GDPR), garanzie adeguate (art. 46 GDPR), norme vincolanti di impresa (art. 47 GDPR), condizioni previste dall'art. 49 GDPR.
11.2. In relazione al presente trattamento, il titolare autorizza il trasferimento dei dati ai Paesi terzi extra-UE indicati nella Sezione A della presente nomina.
11.2.1. Per tutti gli altri trattamenti, non previsti all'interno di tale atto di nomina, spetta al responsabile effettuare una specifica richiesta ed al titolare rilasciare apposita autorizzazione.

12. Violazioni di sicurezza

12.1 Se dovesse venire a conoscenza di una violazione sulla sicurezza dei dati personali, il responsabile, senza ingiustificato ritardo e nel più breve tempo possibile, dovrà: a) informare per iscritto il titolare del trattamento; b) adottare misure ragionevoli per limitare i possibili danni alla sicurezza dei dati personali e comunicarle al titolare; c) fornire al titolare, per quanto possibile, una descrizione della natura della violazione di sicurezza e degli eventuali impatti che questa può avere.
12.2. La comunicazione di una violazione di sicurezza o l'adozione di misure ragionevoli per limitare i possibili danni alla sicurezza dei dati non costituisce riconoscimento di inadempimento o responsabilità da parte del responsabile o dei suoi sub-responsabili.
12.3. Il titolare si impegna a comunicare, senza ingiustificato ritardo e nel più breve tempo possibile, eventuali violazioni di sicurezza riguardanti i servizi offerti dal responsabile.

13.Violazione dei dati

13.1. Se dovesse venire a conoscenza di una violazione dei dati personali (cd. *data breach*), il responsabile, senza ingiustificato ritardo e nel più breve tempo possibile, dovrà informare per iscritto il titolare del trattamento affinché questi possa procedere, se del caso a: a) notificare la violazione all'autorità di controllo competente (art.33 GDPR); b) darne comunicazione agli interessati (art.34 GDPR).
13.2. Il responsabile dovrà aiutare il titolare del trattamento a documentare per iscritto la violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio. Nello specifico dovranno essere documentati: a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) il nome e i dati di contatto del DPO/RPD (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni; c) la descrizione delle probabili conseguenze della violazione dei dati personali; d) le descrizioni delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.
13.3. La comunicazione di una violazione dei dati personali o l'adozione di misure ragionevoli per gestire una violazione dei dati non costituisce riconoscimento di inadempimento o responsabilità da parte del responsabile o dei suoi sub-responsabili.
13.4. Il titolare si impegna a comunicare, senza ingiustificato ritardo e nel più breve tempo possibile, eventuali violazioni dei dati riguardanti i servizi offerti dal responsabile.

14. Responsabilità e risarcimento

14.1. Ai sensi dell'art. 82.2 GDPR, il responsabile del trattamento risponde per danno causato dal trattamento solo se non ha adempiuto gli obblighi del GDPR specificamente diretti al responsabile o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
14.2. Ai sensi dell'art. 82.3 GDPR, il responsabile del trattamento è esonerato dalla responsabilità, a norma dell'art. 82.2 GDPR, se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

15. Altri adempimenti

15.1. Il responsabile del trattamento è tenuto altresì a: a) cooperare con l'Autorità di Controllo quando richiesto; b) supportare l'attività svolta dal DPO/RPD (*Data ProtectionOfficer* – Responsabile della Protezione dei Dati) per conto del titolare del trattamento, se nominato (artt. 37, 38 GDPR).

SEZIONE C
MISURE DI SICUREZZA

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate ad assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.
Qualora vi fosse la possibilità di integrare il prodotto con applicativi di terze parti, CBIM non è responsabile dell'applicazione delle misure di sicurezza relative alle componenti delle terze parti ovvero del funzionamento del prodotto successivamente a tale integrazione.

Da compilarsi a cura del legale rappresentante del titolare del trattamento	
Nome Cognome Codice Fiscale	Laura Figorilli FGRLRA64R65H282N
Data e luogo	
Firma	Firmato digitalmente da: Laura Figorilli Data: 09/04/2024 16:01:52

Da compilarsi a cura del legale rappresentante del responsabile del trattamento	
Nome Cognome Codice Fiscale	PAOLO LUIGI CRISTIANI CRS PLG 56M19 F205L
Data e luogo	
Firma	Firmato digitalmente da: PAOLO LUIGI CRISTIANI Luogo: Pavia Data: 10/04/2024 16:23:24

SISTEMA SANITARIO REGIONALE
IRCCS
ISTITUTI FISIOTERAPICI
OSPITALIERI

IRE
ISTITUTO NAZIONALE TUMORI
REGINA ELENA
ISG
ISTITUTO DERMATOLOGICO
SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

CONTRATTO DI INDIVIDUAZIONE DEL RESPONSABILE DEL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N.679

Gli IRCCS Istituti Fisioterapici Ospitalieri IFO – Istituto Dermatologico Santa Maria e San Gallicano ISG, con sede legale in Via Elio Chianesi, 53 – 00144 Roma, Codice Fiscale 02153140583, Partita Iva 01033011006, nella persona del legale rappresentante *f.f.* Dott.ssa Laura Figorilli, di seguito indicata come DATA CONTROLLER/TITOLARE

e

CBIM – Consorzio di Bioingegneria e Informatica Medica (in seguito "CBIM"), con sede legale in Piazzale Volontari del Sangue n. 2 – 27100 Pavia (IT) - P.IVA 01515320180, nella persona del legale rappresentante pro-tempore, di seguito DATA PROCESSOR/RESPONSABILE

Di seguito, quando indicate congiuntamente, le "Parti"

PREMESSO CHE

a) Il 4 maggio 2016 è stato pubblicato in Gazzetta Ufficiale Europea il Regolamento generale per la protezione dei dati personali – Regolamento UE 2016-679 (anche GDPR);
b) Il Regolamento UE 2016/679 è entrato in vigore il 24 maggio 2016 ed è effettivamente applicabile a partire dal 25 maggio 2018;
c) Il 19 settembre 2018 è entrato in vigore il D.lgs. 101/2018 che ha introdotto le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679;
d) L'art. 28 GDPR prevede che il Titolare del trattamento, individuato ai sensi dell'art. 4 n. 7 GDPR, possa avvalersi di uno o più Responsabili del trattamento dei dati che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di tale Regolamento e garantisca la tutela dei diritti dell'interessato;
e) Il Titolare è stato ammesso quale Ente Partecipante a CBIM e nell'ambito di tale rapporto CBIM svolge per esso il servizio di consulenza per il caricamento dati sul Workflow della Ricerca del Ministero della Salute, come da documentazione richiamata nella richiesta di adesione quale Ente Partecipante a suo tempo trasmessa a CBIM, alla quale si fa integrale rinvio*;*
f) Tale servizio affidato a CBIM comporta il trattamento di dati personali di cui gli IRCCS Istituti Fisioterapici Ospitalieri IFO – Istituto Dermatologico Santa Maria e San Gallicano ISG è Titolare;
g) All'interno della **sezione A** del presente documento, oltre all'indicazione del DPO/RPD designato dal responsabile, sono descritte, in relazione all'attività svolta dal responsabile per conto del titolare: le categorie di trattamento, il tipo di dati personali, le categorie di interessati, l'eventuale trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali e le garanzie adottate, gli eventuali sub-responsabili ed il servizio a questi affidato;
h) All'interno della **Sezione B** del presente documento, sono indicati gli obblighi specifici del responsabile in relazione al trattamento effettuato per conto del titolare del trattamento;
i) All'interno della **Sezione C** del presente documento, sono indicate le misure di sicurezza che il responsabile è tenuto a mettere in atto per garantire un livello di sicurezza adeguato al rischio del trattamento dati effettuato per conto del titolare del trattamento;
j) Ai sensi dell'art. 4 GDPR, per trattamento si intende *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l' adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*;
k) alla luce delle verifiche documentali effettuate, CBIM possiede l'esperienza, la capacità, l'affidabilità e fornisce idonee garanzie del pieno rispetto delle disposizioni vigenti in materia di trattamento dati, ivi compreso il profilo della sicurezza in relazione alle finalità e alle

modalità delle operazioni di trattamento nonché alle garanzie di tutela dei diritti dell'interessato;

l) le parti intendono regolare, con il presente atto, i loro reciproci rapporti in tema di disciplina del trattamento dei dati personali.

Tutto ciò premesso, che costituisce parte integrante del presente atto, DATA CONTROLLER individua ai sensi dell'art. 28 GDPR

CBIM – Consorzio di Bioingegneria e Informatica Medica (in seguito "CBIM"), con sede legale in Piazzale Volontari del Sangue n. 2 – 27100 Pavia (IT) - P.IVA 01515320180

quale Responsabile del trattamento dei dati personali in relazione al trattamento dei dati personali effettuato in forza del contratto sopracitato.

CONTRATTO DI NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

1. OGGETTO E MATERIA

1.1. Con la stipula del presente atto, ai sensi dell'articolo 28 GDPR, il titolare designa CBIM "responsabile" delle operazioni di trattamento dei dati personali affidati. In virtù di tale nomina e del rapporto associativo intercorrente tra le Parti, il responsabile è autorizzato al trattamento dei dati per conto del titolare, così come descritto nel presente documento e nelle sezioni che lo compongono.

1.2. Il contenuto del presente atto, in quanto compatibile, si applica anche ai trattamenti effettuati dagli IRCCS Istituti Fisioterapici Ospitalieri IFO – Istituto Dermatologico Santa Maria e San Gallicano ISG quale responsabile per conto di un titolare terzo rispetto al cui trattamento CBIM si configura quale sub-responsabile. Le parti si riservano di integrare ovvero sostituire il presente atto qualora necessario.

2. OBBLIGHI DEL RESPONSABILE

2.1. La sottoscrizione del presente atto vincola il responsabile del trattamento al titolare del trattamento e fa sorgere in capo al responsabile una serie di obblighi specificamente individuati nella **Sezione B** del presente documento.

3. MISURE DI SICUREZZA E VIOLAZIONE DEI DATI

3.1. Il responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR). Si veda la **Sezione C** del presente documento.

4. DECORRENZA, DURATA, CESSAZIONE DEL TRATTAMENTO

4.1. Il ruolo e le competenze assegnate al responsabile del trattamento con il presente atto hanno la medesima durata ed efficacia della partecipazione, quale Ente Partecipante, del Titolare a CBIM e pertanto si intendono tacitamente rinnovate ogni anno fino alla cessazione della qualifica stessa o fino alla revoca da parte del titolare.

4.2. Dopo il completamento del trattamento per conto del titolare, il responsabile deve, su istruzione del titolare del trattamento, restituire o cancellare i dati personali e le relative copie esistenti, salvo che non siano previste specifiche e differenti politiche di conservazione dei dati (anche in relazione alle categorie di dati trattati) a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento.

4.2.1. Il responsabile deve rilasciare contestualmente un'attestazione scritta che presso lo stesso non esiste alcuna copia dei dati personali trattati in nome e per conto del titolare del trattamento.

5. COMUNICAZIONI TRA LE PARTI

5.1. Le comunicazioni tra le parti, ai fini del presente incarico, dovranno avvenire:

-per il titolare, a dirsci.isg@ifo.it

- per il responsabile, a amministrazione@cbim.it

6. DISPOSIZIONI VARIE

6.1. Il corrispettivo per il presente incarico di responsabile del trattamento rimane ad ogni effetto ricompreso nella quota annuale associativa versata dal Titolare a CBIM in quanto Ente Partecipante.

6.2. Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

6.3. I termini utilizzati all'interno del presente atto hanno lo stesso significato dalla GDPR e dal D. Lgs.

196/2003.
6.3.1. Il presente atto deve essere letto e interpretato secondo quanto disposto dalla GDPR e dal D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018).
6.4. Con l'occasione, il titolare ricorda l'importanza delle prescrizioni di legge in materia di trattamento dei dati personali, nonché il fatto che la violazione di dette normative può comportare responsabilità sia civili che penali per il titolare e per il responsabile, con possibile applicazione di sanzioni amministrative e pecuniarie, ai sensi degli artt. 82, 83 e 84 GDPR.
6.5. Il presente contratto sostituisce qualsiasi altro accordo, contratto o intesa tra le Parti con riferimento al suo oggetto nonché qualsiasi altra istruzione fornita in precedenza, in qualsiasi altra forma, dal titolare al responsabile. Pertanto, in caso di conflitto tra le disposizioni del presente atto e quelle contenute nel Contratto, prevalgono le disposizioni del presente atto.
6.6. Alla cessazione del rapporto associativo per qualsiasi causa, continueranno ad avere efficacia quelle clausole che per loro natura sopravvivono all'estinzione del rapporto giuridico.
6.7. Il Titolare si riserva il diritto di apportare, in qualsiasi momento, tutte le modifiche ed integrazioni al presente atto d'incarico funzionali al miglior rispetto delle disposizioni della Normativa sulla protezione dei dati personali ovvero delle indicazioni o dei provvedimenti del Garante per la protezione dei dati personali o della magistratura ordinaria.
6.7.1. Le variazioni al presente atto d'incarico, intervenute a norma del precedente punto, saranno efficaci per le Parti dopo che la copia aggiornata dello stesso atto sarà stata sottoscritta da entrambe.
6.8. Il titolare dichiara fin da adesso che i dati personali trasmessi al responsabile sono stati raccolti e trattati legittimamente, sono pertinenti e non eccedenti rispetto alle finalità per cui sono stati raccolti e successivamente trattati, che gli interessati sono stati informati di tale trasmissione e che sussiste un'idonea base giuridica che consente al responsabile di effettuare il trattamento dei dati oggetto del presente contratto di nomina.
6.9. Il presente atto di nomina è soggetto alla legge italiana.
6.9.1. Per qualsiasi controversia riguardante la sua applicazione e/o interpretazione è competente in via esclusiva il Foro di Pavia.

SEZIONE A
TRATTAMENTO EFFETTUATO DAL RESPONSABILE PER CONTO DEL TITOLARE

DATI DI CONTATTO DEL RESPONSABILE PROTEZIONE DEI DATI (RPD/DPO) DEL RESPONSABILE DEL TRATTAMENTO (se nominato): dpo.sicurdata@opendata.it; 055750808

Categorie di trattamento	Tipo di dati personali	Categorie di interessati	Trasferimento verso Paesi terzi o organizzazioni internazionali e garanzie adottate	Sub-responsabili e servizi affidati
Trattamenti necessari all'erogazione dell'attività di caricamento dati sul sistema Workflow della Ricerca	Anagrafici, contrattuali, stipendiali	Ricercatori	Non previsto	Consulenti per attività sistemistica e consulenza applicativa

DATI DI CONTATTO DEL RESPONSABILE PROTEZIONE DEI DATI (RPD/DPO) DEL TITOLARE DEL TRATTAMENTO (se nominato): Scudo Privacy S.r.l., nella persona del Dott. Carlo

Villanacci, e-mail: dpo@scudoprivacysrl.com

SEZIONE B
OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO DESIGNATO

In virtù dell'atto che vincola il responsabile designato al Titolare del trattamento, sorgono in capo al responsabile una serie di obblighi.

1. Rispetto delle istruzioni impartite dal titolare

1.1. Il responsabile deve assistere e coadiuvare il titolare nella corretta gestione delle operazioni di trattamento che dovranno essere effettuate nel pieno rispetto degli obblighi previsti dal GDPR e dal D. lgs.196/2003 così come modificato dal D. lgs. 101/2018.

1.2. A tale proposito, il responsabile deve trattare i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un Paese terzo o un'Organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile deve informare il titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

2. Riservatezza

2.1. Il responsabile deve assicurare per sé stesso e per le persone che operano presso la propria azienda, da lui o dal titolare del trattamento autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate.

2.2. Sarà cura del responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il responsabile, in relazione alle operazioni di trattamento da essi eseguite.

3. Conformità a leggi e regolamenti applicabili

3.1. Il responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e del D. lgs. 196/2003 così come modificato dal D. lgs. 101/2018 e, più in generale, ad ogni altra disposizione normativa, nazionale e sovranazionale, in materia di trattamento dei dati personali attualmente in vigore o che in futuro vengano a modificare, integrare o sostituire l'attuale disciplina, nonché ai provvedimenti dell'Autorità Garante competente e alle linee guida adottate dall'*European Data Protection Board*.

4. Misure di sicurezza

4.1. Il responsabile è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR).

4.1.1. A tal proposito, si veda la Sezione C del presente documento.

5. Audit

5.1. Il titolare ha diritto di effettuare audit indipendenti per verificare la conformità del responsabile agli obblighi previsti nel presente contratto ed agli adempimenti in materia di protezione dei dati personali.

5.1.1. In tal caso il titolare dovrà previamente inviare richiesta scritta al responsabile e le Parti concorderanno, almeno dieci giorni prima di quando verrà effettuata la verifica, l'oggetto dei controlli e le relative modalità.

5.2. Titolare e responsabile stabiliranno i vincoli di riservatezza a cui devono essere vincolate le Parti e, eventualmente, coloro che effettueranno le verifiche per conto delle Parti stesse.

5.3. Il responsabile deve contribuire alle attività di revisione, comprese le ispezioni, e ad informare prontamente il titolare del trattamento di ogni questione rilevante ai fini del presente contratto quali, a titolo indicativo: istanze degli interessati, richieste del Garante, esiti delle ispezioni, violazioni del GDPR o di altre disposizioni relative alla protezione dei dati.

5.4. Resta inteso che il Titolare avrà la facoltà di incaricare dei professionisti indipendenti per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report ("Report").

5.4.1. Tali Report, che costituiscono informazioni confidenziali, dovranno essere resi disponibili al Responsabile/Subresponsabile per consentirgli di verificare le eventuali azioni correttive da implementare in funzione al presente Atto.

5.4.2. Il Responsabile potrà opporsi per iscritto alla nomina da parte del Titolare di eventuali revisori esterni che siano concorrenti del Responsabile.
5.4.2.1. In tali circostanze, il Titolare sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.
5.4.2.2. Restano a carico esclusivo del Titolare i costi delle attività di verifica dallo stesso commissionate a terzi.

6. Persone autorizzate al trattamento

6.1. Il responsabile, ai sensi dell'art. 29 GDPR e dell'art. 2 *quaterdecies* D. Lgs. 196/2003, si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, alle quali fornisce specifiche istruzioni scritte (salvo che il diritto dell'Unione o degli Stati membri non richieda diversamente, art. 29 GDPR).
6.2. È compito del responsabile designato vigilare sulla corretta esecuzione delle istruzioni impartite.

7. Sub-responsabile

7.1. Il titolare del trattamento autorizza il responsabile del trattamento a ricorrere ai cd. "sub-responsabili" del trattamento indicati nella sezione A per l'esecuzione delle attività di trattamento ivi descritte.
7.2. Il responsabile inoltra al titolare, qualora questo ne faccia richiesta, l'atto di nomina dei sub-responsabili.
7.3. Il responsabile deve informare il titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili, alle quali il titolare del trattamento conserva il diritto di opporsi.
7.4. Al "sub-responsabile" sono imposti, con specifico atto sottoscritto, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto che lega il titolare e il responsabile del trattamento. Il sub-responsabile è tenuto a: osservare, valutare e organizzare la gestione del trattamento dei dati personali e la loro protezione affinché questi siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "*non gli è in alcun modo imputabile*" (artt. 82. 1 e 82. 3 GDPR).
7.5. Qualora il sub-responsabile abbia necessità di ricorrere ad ulteriori sub-responsabili, lo comunicherà al responsabile che, a sua volta, inoltrerà tale comunicazione al titolare. Il titolare conserva il diritto di opporsi a tali aggiunte.

8. Registro dei Trattamenti

8.1. Il responsabile deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del titolare del trattamento (art. 30 GDPR).
8.2. Il registro, anche in formato elettronico, deve contenere tutta le informazioni descritte dall'art. 30.2 GDPR.
8.3. Il responsabile del trattamento deve mettere il registro a disposizione dell'Autorità di controllo, se questa ne fa richiesta, affinché possa fungere da strumento per il monitoraggio dei trattamenti effettuati.

9. Esercizio dei diritti dell'interessato

9.1. Il responsabile dovrà informare, tempestivamente e per iscritto, il titolare del trattamento della ricezione di eventuali richieste degli interessati, avanzate ai sensi degli artt. da 15 a 22 del GDPR, ovvero al fine di revocare il consenso prestato e/o proporre reclamo al Garante per la protezione dei dati personali.

10. Valutazione d'impatto sulla protezione dei dati

10.1. Il responsabile del trattamento, se necessario e su richiesta del titolare, dovrà fornire a questi le informazioni necessarie per consentirgli di effettuare la valutazione di impatto ai sensi dell'art. 35 GDPR.

11. Trasferimento dei dati personali all'estero.

11.1. Al Responsabile è fatto divieto di trasferire i dati personali trattati per conto del titolare a Paesi Extra-UE in assenza di un'autorizzazione da parte del titolare e in assenza di: una decisione di adeguatezza (art. 45 GDPR), garanzie adeguate (art. 46 GDPR), norme vincolanti di impresa (art. 47 GDPR), condizioni previste dall'art. 49 GDPR.

11.2. In relazione al presente trattamento, il titolare autorizza il trasferimento dei dati ai Paesi terzi extra-UE indicati nella Sezione A della presente nomina.
11.2.1. Per tutti gli altri trattamenti, non previsti all'interno di tale atto di nomina, spetta al responsabile effettuare una specifica richiesta ed al titolare rilasciare apposita autorizzazione.

12. Violazioni di sicurezza

12.1 Se dovesse venire a conoscenza di una violazione sulla sicurezza dei dati personali, il responsabile, senza ingiustificato ritardo e nel più breve tempo possibile, dovrà: a) informare per iscritto il titolare del trattamento; b) adottare misure ragionevoli per limitare i possibili danni alla sicurezza dei dati personali e comunicarle al titolare; c) fornire al titolare, per quanto possibile, una descrizione della natura della violazione di sicurezza e degli eventuali impatti che questa può avere.
12.2. La comunicazione di una violazione di sicurezza o l'adozione di misure ragionevoli per limitare i possibili danni alla sicurezza dei dati non costituisce riconoscimento di inadempimento o responsabilità da parte del responsabile o dei suoi sub-responsabili.
12.3. Il titolare si impegna a comunicare, senza ingiustificato ritardo e nel più breve tempo possibile, eventuali violazioni di sicurezza riguardanti i servizi offerti dal responsabile.

13.Violazione dei dati

13.1. Se dovesse venire a conoscenza di una violazione dei dati personali (cd. *data breach*), il responsabile, senza ingiustificato ritardo e nel più breve tempo possibile, dovrà informare per iscritto il titolare del trattamento affinché questi possa procedere, se del caso a: a) notificare la violazione all'autorità di controllo competente (art.33 GDPR); b) darne comunicazione agli interessati (art.34 GDPR).
13.2. Il responsabile dovrà aiutare il titolare del trattamento a documentare per iscritto la violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.Nello specifico dovranno essere documentati: a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) il nome e i dati di contatto del DPO/RPD (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni; c) la descrizione delle probabili conseguenze della violazione dei dati personali; d) le descrizioni delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.
13.3. La comunicazione di una violazione dei dati personali o l'adozione di misure ragionevoli per gestire una violazione dei dati non costituisce riconoscimento di inadempimento o responsabilità da parte del responsabile o dei suoi sub-responsabili.
13.4. Il titolare si impegna a comunicare, senza ingiustificato ritardo e nel più breve tempo possibile, eventuali violazioni dei dati riguardanti i servizi offerti dal responsabile.

14. Responsabilità e risarcimento

14.1. Ai sensi dell'art. 82.2 GDPR, il responsabile del trattamento risponde per danno causato dal trattamento solo se non ha adempiuto gli obblighi del GDPR specificamente diretti al responsabile o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
14.2. Ai sensi dell'art. 82.3 GDPR, il responsabile del trattamento è esonerato dalla responsabilità, a norma dell'art. 82.2 GDPR, se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

15. Altri adempimenti

15.1. Il responsabile del trattamento è tenuto altresì a: a) cooperare con l'Autorità di Controllo quando richiesto; b) supportare l'attività svolta dal DPO/RPD (*Data ProtectionOfficer* – Responsabile della Protezione dei Dati) per conto del titolare del trattamento, se nominato (artt. 37, 38 GDPR).

SEZIONE C
MISURE DI SICUREZZA

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate ad assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.
Qualora vi fosse la possibilità di integrare il prodotto con applicativi di terze parti, CBIM non è responsabile dell'applicazione delle misure di sicurezza relative alle componenti delle terze parti ovvero del funzionamento del prodotto successivamente a tale integrazione.

Da compilarsi a cura del legale rappresentante del titolare del trattamento	
Nome Cognome Codice Fiscale	Laura Figorilli FGRLRA64R65H282N
Data e luogo	
Firma	Firmato digitalmente da: Laura Figorilli Data: 09/04/2024 16:28:28

Da compilarsi a cura del legale rappresentante del responsabile del trattamento	
Nome Cognome Codice Fiscale	PAOLO LUIGI CRISTIANI CRS PLG 56M19 F205L
Data e luogo	
Firma	Firmato digitalmente da: PAOLO LUIGI CRISTIANI Luogo: Pavia Data: 10/04/2024 16:28:33