Prot. n. 0014246 del 17/01/2024 - UOR: 86

ACCORDO QUADRO

tra

Consiglio Nazionale delle Ricerche (nel seguito "**CNR**"), C.F. 80054330586, con sede in Roma, Piazzale Aldo Moro n. 7, rappresentato da Prof.ssa Maria Chiara Carrozza, in qualità di Presidente e legale rappresentante, domiciliato per la carica presso la sede dello stesso CNR,

e

Fondazione Istituto Italiano di Tecnologia (nel seguito "**IIT**"), C.F. 97329350587, con sede legale in Genova, Via Morego n. 30, nella persona del suo Direttore Scientifico, Prof. Giorgio Metta, debitamente autorizzato alla firma del presente atto,

Nel seguito anche, individualmente, "Parte" e, congiuntamente, "Parti"

Premesso che:

- Il CNR, in base al suo Statuto, è un Ente pubblico nazionale di ricerca con competenza scientifica generale con il compito di svolgere, promuovere, diffondere, trasferire e valorizzare attività di ricerca nei principali settori di sviluppo delle conoscenze e delle loro applicazioni per lo sviluppo scientifico, tecnologico, economico e sociale del Paese, perseguendo l'integrazione di discipline e tecnologie diffusive ed innovative anche attraverso accordi di collaborazione e programmi integrati;
- Il CNR svolge, promuove e coordina attività di ricerca con obiettivi di eccellenza in ambito nazionale e internazionale, finalizzate all'ampliamento delle conoscenze nei principali settori di sviluppo, individuati nel quadro della cooperazione ed integrazione europea e della collaborazione con le università e con altri soggetti sia pubblici sia privati;
- Il CNR, per lo svolgimento delle proprie attività istituzionali e di ogni altra attività connessa, ivi compreso l'utilizzo economico dei risultati della ricerca propria e di quella commissionata, secondo criteri e modalità determinati con il regolamento di organizzazione e funzionamento, può:
  a) stipulare accordi e convenzioni con soggetti pubblici e privati, sia nazionali che internazionali;
  b) partecipare o costituire consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri, previa autorizzazione del Ministro dell'Istruzione, dell'Università e della Ricerca;

c) promuovere l'inserimento nel settore della ricerca di giovani ricercatori sia per il conseguimento dei propri obiettivi istituzionali sia per la crescita complessiva del patrimonio umano ai fini di una maggiore competitività del paese e dei territori;
d) svolgere un ruolo importante nel formare ricercatori destinati non solo ad essere ammessi nella propria rete scientifica e promuove la formazione dei giovani ricercatori anche attraverso l'assegnazione di borse di studio;
e) commissionare attività di ricerca e studio a soggetti pubblici e privati, nazionali e internazionali;

- In base al vigente regolamento di organizzazione e funzionamento del CNR, i rapporti di collaborazione nell'attività di ricerca tra il CNR ed i soggetti pubblici e privati sono regolati da Accordi Quadro che definiscono aree progettuali, modalità di collaborazione e costituiscono la base per la successiva stipula di convenzioni operative;
- IIT è una Fondazione senza scopo di lucro il cui principale obiettivo è promuovere l'eccellenza nella ricerca di base e applicata. Il Programma Scientifico di IIT è contraddistinto da una marcata multidisciplinarietà, con competenze in 4 ambiti principali di ricerca: Robotica, Nanomateriali, Tecnologie per le Scienze della Vita e Scienze Computazionali;
- nel corso del 2009 IIT e CNR hanno sottoscritto un protocollo d'intesa di durata quinquennale (prot. IIT n. 14982/09 e prot. CNR n. 67414 del 29.09.2009) volto a favorire lo sviluppo di programmi di ricerca in collaborazione, al quale hanno fatto seguito accordi specifici, tuttora in corso di vigenza, tra IIT e diversi istituti del CNR quali: Istituto di Biologia e Biotecnologia Agraria (CNR-IBBA), Istituto di Matematica Applicata e Tecnologie Informatiche "E. Magenes" (CNR-IMATI), Istituto di Nanotecnologia (CNR-NANOTEC) e Istituto per la Microelettronica e Microsistemi (CNR-IMM).

Considerate, inoltre, le proficue relazioni già instaurate, le Parti manifestano interesse a proseguire la collaborazione al fine di programmare, promuovere e intraprendere attività di ricerca, formazione avanzata e divulgazione scientifica in tutti i settori di comune interesse e, più in generale, nei rispettivi campi di azione specifici mediante la sottoscrizione del presente accordo quadro (di seguito, l'"Accordo Quadro").

Tra le Parti sopra costituite si conviene e si stipula quanto segue:

ART. 1 – Premesse

Le premesse costituiscono parte integrante del presente Accordo Quadro.

ART. 2 – Oggetto e finalità

2.1 Le Parti, nell'ambito dei rispettivi compiti e funzioni attribuite per legge, cooperano per l'individuazione e lo sviluppo di un portafoglio di programmi di ricerca, formazione, trasferimento tecnologico ed altre iniziative comuni in tutti i settori di comune interesse. Le modalità e le forme di collaborazione saranno regolate attraverso la stipula di specifiche convenzioni operative adottate sulla base dell'art. 5 del presente Accordo Quadro ed ai sensi degli ordinamenti interni delle Parti.

ART. 3 – Tipologia delle azioni programmatiche

3.1 Le azioni programmatiche poste in essere dalle Parti potranno riguardare principalmente:

- l'esecuzione di progetti congiunti di ricerca;
- la valorizzazione e divulgazione di conoscenze tecnico-scientifiche;
- la realizzazione di infrastrutture di ricerca;
- la sottomissione congiunta di progetti di ricerca/*proposal* presso enti finanziatori;
- l'accesso di personale dipendente, collaboratori e studenti ai rispettivi laboratori e strutture di ricerca.

3.2 Per la realizzazione delle predette iniziative, le Parti intendono promuovere un processo di collaborazione attraverso il quale risorse qualificate del CNR e di IIT potranno effettuare esperienze significative presso le strutture firmatarie del presente Accordo Quadro. A tal fine le Parti, sulla base delle rispettive disponibilità, contribuiranno con le risorse necessarie e secondo le modalità previste dalle convenzioni operative indicate nell'art. 5.

ART. 4 - Responsabili dell'Accordo Quadro

Le Parti individuano come responsabili del presente Accordo Quadro:

- per IIT: il Direttore Scientifico, Prof. G. Metta;

- per CNR: il Direttore f.f. di ISTI-CNR, Dott. Roberto Scopigno

con il compito di dare risalto al presente Accordo Quadro, favorendo quanto più possibile le azioni programmatiche elencate all'art. 3, nonché le proposte di stipula di specifiche convenzioni operative di cui al successivo art. 5, che dovranno essere approvate sulla base dei rispettivi regolamenti interni delle Parti.

ART. 5 – Convenzioni operative

5.1 Le modalità concernenti l'esecuzione del presente Accordo Quadro saranno definite all'atto della stipula delle convenzioni operative (di seguito, le "Convenzioni Operative").
Le Convenzioni Operative dovranno contenere descrizioni e previsioni specifiche relative a: a) attività da svolgere; b) obiettivi da realizzare; c) termini e condizioni di svolgimento; d) tempi di attuazione; e) risorse umane e strumentali da impiegare e messe a disposizione dalle Parti; f) definizione degli eventuali oneri finanziari relativi alle singole attività tecnico-scientifiche e delle loro modalità di erogazione; g) regime dei risultati scientifici e disciplina dei diritti di proprietà intellettuale applicabile, nonché – laddove necessario - alla riservatezza di specifiche informazioni scambiate nell'ambito e ai fini delle attività di ricerca concordate; h) procedure di accesso del personale di ciascuna Parte presso le sedi dell'altra Parte; i) trattamento dei dati personali che dovessero risultare dall'esecuzione del presente Accordo Quadro e le relative misure di sicurezza da adottare.

5.2 Le attività disciplinate dalle Convenzioni Operative avranno inizio secondo la tempistica concordata tra le Parti, che valuteranno le priorità in relazione ai rispettivi programmi di ricerca.

5.3 Alla Convenzione Operativa possono aderire eventuali altri soggetti che intendono contribuire con proprie risorse all'attuazione del progetto congiunto oggetto della stessa.

Art. 6 – Risorse

6.1 Il presente Accordo Quadro non comporta oneri finanziari per le Parti.
Le Parti sosterranno, compatibilmente con le disponibilità di bilancio e con le proprie risorse finanziarie, i costi di realizzazione delle attività di ricerca congiunte secondo le modalità disciplinate dalle Convenzioni Operative di cui all'art. 5.
6.2 Ulteriori risorse potranno essere messe a disposizione delle Parti a seguito di finanziamenti provenienti dal Ministero per l'Istruzione, l'Università e la Ricerca, dal Ministero dello Sviluppo Economico, dalla Commissione Europea, da altri Ministeri, Regioni ed altri soggetti interessati.

Art. 7 – Proprietà Intellettuale e Riservatezza

7.1 Ciascuna Parte è e rimane titolare delle conoscenze, del *know-how* e delle informazioni di cui era già titolare prima della sottoscrizione del presente Accordo Quadro, nonché di tutti i diritti di proprietà intellettuale ad essi relative (di seguito "*Background*"), e che ha reso disponibili all'altra Parte in occasione delle attività oggetto del presente Accordo Quadro e delle eventuali successive Convenzioni Operative. Il *Background* costituisce Informazione Confidenziale della Parte che lo mette a disposizione dell'altra al fine dell'esecuzione delle attività congiunte, e dovrà, pertanto, essere trattato in conformità con quanto disposto al successivo comma 2. Resta espressamente inteso che, con il presente Accordo Quadro, le Parti non concedono né trasferiscono alcun diritto, neanche implicito, a favore dell'altra Parte, in relazione al proprio *Background*.
Come stabilito al precedente art. 5 comma 1, le Parti regoleranno nelle singole Convenzioni Operative la titolarità dei risultati delle attività svolte e le modalità di loro gestione, eventuale protezione e valorizzazione, anche in considerazione di eventuali condizioni poste da soggetti finanziatori di progetti congiunti, restando in ogni caso inteso che ciascuna Parte si dovrà adoperare al fine di acquisire o comunque detenere la titolarità dei risultati e dei diritti di proprietà intellettuale insistenti sui medesimi, in modo da poterne disporre nelle modalità che verranno stabilite dalle Parti nelle Convenzioni Operative.

7.2 Le Parti prendono atto che, nell'ambito del presente Accordo Quadro e al fine della realizzazione delle Convenzioni Operative, ciascuna Parte potrà avere accesso o venire a conoscenza di informazioni, dati o conoscenze dell'altra Parte o comunque in suo legittimo possesso, di carattere tecnico, scientifico, commerciale, o di qualunque altra natura, di carattere riservato e segreto ("Informazioni Confidenziali"). Pertanto, ciascuna Parte si impegna fin da ora a:
(i) utilizzare le Informazioni Confidenziali nella misura e con i mezzi strettamente necessari allo svolgimento delle attività oggetto del presente Accordo Quadro e delle Convenzioni Operative, e con modalità che non ne compromettano in alcun modo il carattere della riservatezza;
(ii) non divulgare o rendere in alcun modo accessibili a qualsiasi terza parte le Informazioni Confidenziali, né in tutto né in parte, direttamente o indirettamente, senza aver prima ottenuto un'autorizzazione scritta della Parte divulgante;

(ii) non utilizzare le Informazioni Confidenziali, né in tutto né in parte, direttamente o indirettamente, per fini diversi da quanto previsto dal presente Accordo Quadro e dalle Convenzioni Operative;
(iii) mettere in atto tutte le misure adeguate a garantire e mantenere la massima riservatezza delle Informazioni Confidenziali, nonché a impiegare la diligenza necessaria a prevenire usi non autorizzati, o divulgazioni interne o esterne indebite; e
(iv) non copiare, duplicare, riprodurre, memorizzare o registrare, con ogni e qualsiasi mezzo a tali fini idoneo, in tutto o in parte, direttamente o indirettamente, file, atti, documenti, disegni, schemi, e ogni altro materiale contenente una o più Informazioni Confidenziali, salvo consenso espresso dalla Parte che ne abbia diritto;
(v) limitare internamente l'accesso alle Informazioni Confidenziali a quei dipendenti, collaboratori o altro personale che, per competenze, funzioni o compiti specifici, si trovino nella necessità di conoscerle ed utilizzarle; tale divulgazione potrà in ogni caso avvenire soltanto a condizione che tali soggetti sottoscrivano un accordo di confidenzialità di contenuto analogo o comunque di portata non minore di quello del presente Accordo Quadro.
La natura riservata delle Informazioni Confidenziali dovrà essere evidenziata mediante indicazione della dicitura "riservato", "confidenziale" o con simile legenda; le informazioni divulgate verbalmente o visivamente dovranno essere identificate dalla parte divulgante come "Informazioni Confidenziali" al momento della loro divulgazione, e la relativa confidenzialità dovrà essere tempestivamente confermata dalla parte divulgante con una comunicazione scritta da trasmettersi alla parte ricevente entro 15 (quindici) giorni dall'avvenuta divulgazione.
Resta inteso che, l'assenza di tali esplicite indicazioni circa la riservatezza, in ogni caso, non precluderà la qualificazione di un'informazione come "Informazione Confidenziale" se il divulgante è in grado di provare la sua natura confidenziale, o se il ricevente conosceva o avrebbe dovuto conoscere la sua natura confidenziale, proprietaria o segreta per il divulgante.
Ciascuna Parte garantisce che il proprio personale, dipendente, consulente e/o collaboratore, destinato allo svolgimento delle attività oggetto del presente Accordo Quadro e delle Convenzioni Operative manterrà nei confronti di qualsiasi terzo non autorizzato la riservatezza per quanto attiene alle Informazioni Confidenziali di cui dovesse venire a conoscenza, nonché per quanto attiene ai risultati conseguiti. A tal fine, ciascuna Parte si impegna sin d'ora a tenere indenne e manlevare l'altra Parte per ogni danno o pregiudizio quest'ultima abbia a subire in connessione e/o in dipendenza con eventuali violazioni delle disposizioni del presente articolo, posti in essere dall'altra Parte e/o dai propri dipendenti, consulenti e/o collaboratori, a meno che la Parte inadempiente non provi che tale violazione si sia verificata nonostante l'uso della migliore diligenza in rapporto alle circostanze.
Gli obblighi di cui al presente articolo 7.2 resteranno validi per la durata del presente Accordo Quadro e per un periodo di 5 (cinque) anni successivo alla data di scadenza o cessazione, per qualsivoglia motivo, dello stesso.

ART. 8 – Tutela dei dati personali

8.1 Le Parti tratteranno i dati personali forniti nello svolgimento del presente Accordo Quadro esclusivamente con il fine di definire l'Accordo Quadro medesimo, secondo quanto previsto dal Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ("Regolamento" o il "RGDP"), sulla base del presupposto normativo definito dall'art. 6, par. 1, lett. b) del Regolamento medesimo e con le modalità e garanzie di cui al D. Lgs. n. 196/2003 ("Codice in materia di protezione

dei dati personali", come modificato dal D. Lgs. 10/08/2018 n. 101 per adeguamento al RGPD).

Le Parti concordano sin d'ora che il trattamento dei dati personali effettuato nell'ambito delle singole Convenzioni Operative avverrà nel rispetto delle misure di sicurezza organizzative di cui all'Allegato 2 "Misure di sicurezza organizzative relative ai dati personali", qui fornito a titolo informativo in forma di facsimile.

8.2 Le Parti si impegnano altresì a definire nelle successive Convenzioni Operative, ruoli ed obblighi relativi ai trattamenti che deriveranno dalle specifiche attività.

ART. 9 – Gestione dei Data Breach

Tenendo conto della natura del trattamento e delle informazioni a disposizione, ciascuna delle Parti si impegna ad informare tempestivamente l'altra Parte, a mezzo PEC, agli indirizzi di ciascuna indicati al seguente articolo 15 (Comunicazioni), inserendo in copia conoscenza l'indirizzo email gdpr@iit.it, ogniqualvolta sia ragionevolmente certa che la violazione che si è verificata nell'ambito delle singole Convenzioni Operative - che costituiscano attuazione presente Accordo Quadro - comporti la compromissione di dati personali (di seguito, "Data Breach"), fermo restando il rispetto degli articoli 33 e 34 del RGPD. Ai sensi dell'articolo 82.2 del RGPD, ciascuna delle Parti è tenuta a rispondere per il danno cagionato dal suo trattamento che violi il Regolamento.

ART. 10 – Sicurezza delle Informazioni

Le Parti concordano sin d'ora che qualunque informazione in formato digitale trattata all'interno delle singole Convenzioni Operative che costituiscano attuazione del presente Accordo Quadro sarà gestita e formalizzata secondo le modalità previste dall'Allegato 1 "Misure di sicurezza tecnico-organizzative ICT", qui fornito a titolo informativo in forma di facsimile.

ART. 11 – Uso dei segni distintivi e visibilità dell'Accordo Quadro

11.1 Il contenuto del presente Accordo Quadro non conferisce alle Parti alcun diritto di usare, per scopi pubblicitari o per qualunque altra attività promozionale, alcun nome, marchio, o altra designazione dell'altra Parte, incluse le abbreviazioni (di seguito, "Segni Distintivi"). Eventuali eccezioni potranno essere pattuite dalle Parti tramite separato accordo scritto. Sono in ogni caso fatti salvi gli usi liberi di legge, ex art. 21 del D. Lgs. n. 30/2005 "Codice della Proprietà Industriale", della sola denominazione in funzione descrittiva, purché resa in forma veritiera.

11.2 Fermo restando quanto sopra, le Parti si concedono reciprocamente l'autorizzazione ad utilizzare i rispettivi Segni Distintivi al solo ed esclusivo fine di dare adeguata visibilità ai contenuti di cui al presente Accordo Quadro, limitatamente alla sua durata. Le Parti, tramite i rispettivi uffici a ciò preposti, definiranno le modalità operative d'utilizzo dei Segni Distintivi. Per quanto concerne IIT, CNR dovrà fare riferimento a roo@iit.it e, per quanto riguarda CNR, IIT dovrà fare riferimento a rpd@cnr.it.

ART. 12 – Durata

12.1 Il presente Accordo Quadro ha la durata di 5 (cinque) anni a decorrere dalla data della sua ultima sottoscrizione e potrà essere rinnovato per un uguale periodo solo mediante ulteriore atto scritto tra le Parti, salvo disdetta da parte di uno dei contraenti da comunicarsi all'altro contraente a mezzo di PEC entro e non oltre 6 (sei) mesi dalla scadenza del presente Accordo Quadro.

12.2 È fatta salva la possibilità per le Parti di provvedere alla sottoscrizione anche a mezzo di firma digitale ai sensi e nel rispetto del D.P.C.M. del 22 febbraio 2013, pubblicato sulla G.U. n. 117 del 21 maggio.

ART. 13 – Modifiche e Recesso

13.1 Qualora, nel corso del quinquennio, venissero a modificarsi i presupposti per i quali si è provveduto alla stipula del presente Accordo Quadro o si ritenesse opportuno rivedere lo stesso, le Parti procederanno di comune accordo e le eventuali modifiche da apportare dovranno rivestire la forma scritta.

13.2 Ciascuna delle Parti avrà la facoltà di recedere dal presente Accordo Quadro senza oneri o corrispettivi, dandone comunicazione scritta all'altra Parte con un preavviso di almeno 90 (novanta) giorni a mezzo di raccomandata A/R e/o PEC.

13.3 In caso di recesso restano salve le eventuali iniziative già avviate congiuntamente, salvo che le Parti di comune accordo non decidano diversamente.

ART. 14 – Nullità parziale

14.1 Qualora qualsivoglia clausola del presente Accordo Quadro sia riconosciuta non valida o di impossibile attuazione, oppure successivamente diventata – totalmente e/o parzialmente – non valida o di impossibile attuazione, ciò non inficia la validità del rimanente dettato del presente Accordo Quadro, fatto salvo quanto previsto dall' art. 1419 del Codice civile.

14.2 Nel caso in cui si verifichi quanto previsto al comma di cui sopra, le Parti provvederanno a concordare una valida clausola sostitutiva che sia il più vicino possibile allo scopo della clausola non valida e/o di impossibile attuazione, al fine di superare la situazione che ne ha determinato l'invalidità e/o la impossibilità di attuazione.

ART. 15 – Comunicazioni

Tutte le comunicazioni relative al presente Accordo Quadro dovranno essere effettuate per iscritto ai seguenti indirizzi o a quelli successivamente indicati con le stesse modalità da una Parte all'altra:

Se a IIT:

Fondazione Istituto Italiano di Tecnologia - Via Morego, 30 – 16163 Genova – Direzione per l'Organizzazione della Ricerca, all'attenzione del Prof. Giorgio Metta - Direttore Scientifico o all'indirizzo PEC: roo@pec.iit.it

Se a CNR:

Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo" – Via Moruzzi, 1 - 56124 Pisa, all'attenzione del Direttore f.f. dott. Roberto Scopigno o all'indirizzo PEC: direttore.isti@pec.cnr.it

ART. 16 – Registrazione

Il presente Accordo Quadro sarà registrato in caso d'uso. Le spese di registrazione saranno a carico della parte richiedente.

ART. 17 – Rinvii e Foro Competente

Per quanto non espressamente previsto dal presente Accordo Quadro si fa rinvio alle norme vigenti in materia. In caso di controversia nell'interpretazione o esecuzione del presente Accordo Quadro, che non si possa risolvere in via amichevole, il Foro competente sarà quello di Roma.

ART. 18 – Adempimenti *ex lege* 231/2001

Il CNR dichiara di essere a conoscenza della normativa vigente in materia di responsabilità amministrativa degli enti e, in particolare, del Decreto Legislativo 8 giugno 2001, n. 231 e di aver preso atto del Codice di Comportamento e di Condotta Scientifica nonché del Modello di Organizzazione, Gestione e Controllo adottati da IIT ai sensi della predetta normativa (disponibili al seguente link: https://www.iit.it/it/web/guest/trasparenza).

ART. 19 – Conflitto di interessi

Le Parti dichiarano di aver adottato tutte le misure atte a prevenire e contrastare il conflitto di interessi e di averle recepite nella propria normativa e documentazione interna e pertanto si impegnano ad applicarle qualora emerga che i soggetti coinvolti a qualunque titolo nell'esecuzione del presente Accordo Quadro e/o delle conseguenti Convenzioni Operative denuncino l'esistenza, anche apparente, di tale conflitto.

Letto, confermato e sottoscritto digitalmente

Consiglio Nazionale delle Ricerche
La Presidente – Prof.ssa Maria Chiara Carrozza

Maria Chiara Carrozza
16.01.2024 19:09:59 GMT+01:00

Fondazione Istituto Italiano di Tecnologia
Il Direttore Scientifico – Prof. G. Metta

Digitally signed by: Giorgio Metta
Date: 22/12/2023 16:16:02

Allegato 1: Misure di sicurezza tecnico-organizzative ICT - Facsimile
Allegato 2: Misure di sicurezza organizzative relative ai dati personali – Facsimile

ALLEGATO 1
MISURE DI SICUREZZA TECNICO-ORGANIZZATIVE ICT - FACSIMILE

1. MISURE DI SICUREZZA

Nel contesto della sicurezza delle informazioni è fondamentale comprendere che il grado di rischio associato ad un trattamento di dati può variare significativamente in base alla natura e alla sensibilità delle informazioni gestite. Ciascuna Parte firmataria dell'Accordo Quadro sottoscritto in data ….. (n. di protocollo …..) deve garantire, per mezzo del Responsabile della Direzione ICT o del Responsabile della Sicurezza delle Informazioni (CISO), come indicato nei paragrafi sottostanti, l'adozione di misure di sicurezza adeguate a proteggere le informazioni in formato digitale trattate all'interno delle Convenzioni Operative che costituiscono attuazione dell'Accordo Quadro sopra identificato.

Le misure di sicurezza riportate nelle tabelle sottostanti, divise in "organizzative" e "tecniche", rappresentano quindi un insieme di linee guida di base minime, riportate a titolo non esaustivo, che dovrebbero essere implementate nei sistemi a perimetro degli accordi operativi che vengono a costituirsi fra le Parti. Pertanto, tali misure devono costituire il punto di partenza e, in caso di trattamenti dei dati considerati ad alto rischio, dovranno essere rivalutate e, se necessario, rafforzate al fine di garantire una protezione adeguata e la conformità alle normative vigenti.

Ciascuna Parte dovrà essere in grado, se richiesto dall'altra Parte, di fornire evidenza della conformità ai controlli selezionati. Nel caso in cui una Parte non sia in grado di soddisfare in tutto o in parte una misura di sicurezza tecnica o non la ritenga applicabile dovrà fornire le necessarie motivazioni ed evidenze circa gli eventuali controlli compensativi adottati.

In caso di ricorso a fornitori (sub-responsabili) per la gestione dei servizi informatici e di sicurezza l'applicazione delle misure sotto descritte dovrà essere traferita contrattualmente ai fornitori stessi. Ciascuna Parte si impegna inoltre a tener traccia dei fornitori coinvolti in un registro apposito, che può essere richiesto dall'altra Parte per verifica e controllo.

Ogni qualvolta si verifichi un incidente di sicurezza che coinvolga le Informazioni trattate, questo dovrà essere comunicato tempestivamente ai contatti individuati nel paragrafo sottostante.

1.1. Contatti dei Responsabili e dei referenti tecnici delle Parti

Responsabile ICT (CIO) e/o Responsabile Sicurezza delle Informazioni (CISO) di XXX

Nome, Cognome ……

Indirizzo e-mail ……

Contatto telefonico …….

Referente tecnico di XXX verso IIT

Come Referente dei controlli di sicurezza organizzativi e tecnici, IIT può fare riferimento a:

Nome, Cognome ……
Indirizzo e-mail ……
Contatto telefonico ……

Responsabile ICT di IIT

Stefano Bencetti (ICT Director)
stefano.bencetti@iit.it
+39 010 2896 505

Referente tecnico di IIT verso XXX

Come Referente dei controlli di sicurezza organizzativi e tecnici, XXX può fare riferimento a:

Nome, Cognome ……
Indirizzo e-mail ……
Contatto telefonico …….

1.2. Misure di sicurezza organizzative

Item #	Categoria	Controllo	Compliance IIT (S/N/n.a.)	Compliance Parte XXX (S/N/n.a.)	Note giustificative (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)
1	Policy di Sicurezza delle Informazioni	L'organizzazione deve documentare la propria politica di sicurezza delle informazioni. La politica di sicurezza deve essere riesaminata e riveduta, se necessario, su base annua. La politica di sicurezza deve almeno riferirsi a: ruoli e responsabilità del personale, ivi inclusa l'individuazione di un responsabile della sicurezza delle informazioni, misure tecniche e organizzative di base adottate per la sicurezza dei dati, i responsabili dei dati o altre terze parti coinvolte nel trattamento di dati. La politica deve essere approvata dalla direzione e comunicata a tutti i dipendenti e alle parti esterne pertinenti.			
2	Sicurezza delle Risorse Umane, Consapevolezza e Formazione	Prima iniziare il rapporto di lavoro ai dipendenti deve essere chiesto di prendere visione del documento o della politica di sicurezza dell'organizzazione e di firmare i rispettivi accordi di riservatezza e di non divulgazione. L'organizzazione deve avere programmi di formazione e			

		sensibilizzazione strutturati e regolari per il personale, compresi programmi specifici relativi alla protezione dei dati. Il piano di formazione deve essere preparato ed eseguito su base annua, o con altra periodicità ritenuta adeguata.			
3	Policy di gestione degli asset	L'organizzazione deve documentare la propria politica per quanto riguarda l'utilizzo delle risorse informatiche aziendali, ivi inclusi i dispositivi mobili e quelli personali.			
4	Policy per il Controllo degli Accessi	Autorizzazioni specifiche per il controllo dell'accesso ai dati devono essere assegnate a ciascun ruolo in seguito alla necessità del rispetto del principio del “need to know”. I criteri di controllo accesso devono essere dettagliati e documentati. L'organizzazione deve documentare le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per ruoli utente specifici verso i processi e le procedure relative ai dati trattati. Il principio della “Segregation of Duty” (ad es. richiesta di accesso, autorizzazione di accesso, amministrazione dell'accesso) deve essere chiaramente definito e documentato.			
5	Gestione degli incidenti relativi alla sicurezza delle informazioni	Deve essere definito e documentato un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti. Il piano deve assicurare che le violazioni dei dati personali siano immediatamente segnalate al Titolare entro gli accordi contrattualizzati.			
6	Conformità alla sicurezza delle	L'organizzazione deve svolgere con cadenza almeno			

	informazioni	annuale una verifica (o audit interno) delle proprie misure tecniche e organizzative per l'implementazione di eventuali azioni correttive. Deve essere eseguita una verifica degli aspetti di security ed implementate le raccomandazioni conseguenti prima dell'utilizzo in produzione di applicazioni che trattano dati personali.			

1.3. Misure di sicurezza tecniche

Gestione degli accessi e delle credenziali

Devono essere applicate misure di sicurezza agli accessi logici, come password robuste (o equivalente codice di protezione per dispositivi mobili) e modifica periodica delle stesse. Deve essere effettuata una revisione periodica dei permessi di accesso, ad esempio in caso di cessazione del rapporto con la Società o di cambiamenti interni all'organizzazione.

Firewall

Deve essere attivato un firewall di rete, che permetta solo il traffico e i servizi necessari.

Inventario

Gli asset gestiti (incluse le applicazioni) devono essere registrati in un inventario con le loro informazioni di rilievo, e mantenuti aggiornati.

Patching

Devono essere usate versioni supportate di applicazioni e sistemi operativi. Le patch di sicurezza classificate come "critiche" e "gravi" devono essere applicate con priorità e secondo un piano definito.

Protezione da Malware

Deve essere installato e tenuto aggiornato un agente antivirus/anti-malware.

Gestione delle vulnerabilità

Deve essere effettuata regolarmente una scansione di vulnerabilità e le vulnerabilità ad alto rischio riscontrate devono essere risolte con priorità secondo un piano definito.

Backup

Deve essere effettuato regolarmente un backup di dati e configurazioni. I dati di backup devono essere cifrati in transito e quando salvati su supporti esterni, e testati per assicurarsi che possano essere usati in caso di necessità.

Sicurezza delle Comunicazioni

Le informazioni trasferite su canali applicativi devono essere cifrate nel trasporto, ad esempio usando protocolli sicuri e non deprecati (TLS, https, ssh) o canali cifrati (VPN).

Cancellazione sicura

Quando non più necessari, i dati devono essere rimossi in maniera permanente con tecniche di cancellazione sicura. Per i device remoti, ciò deve poter essere controllato centralmente.

Cifratura

Deve essere prevista la cifratura delle unità d'archiviazione, quali dischi rigidi (in particolare dei laptop), dischi e chiavette USB, DVD, backup tapes, ecc. Per i file, i record o i campi più critici devono essere considerate soluzioni di cifratura, adottandole ove possibile.

Gestione dei log

I log, inclusi quelli degli Amministratori di Sistema, devono essere inviati ad un sistema di raccolta centrale, che ne prevenga l'alterazione. Per le applicazioni cloud, tali log devono essere resi disponibili ed esportabili su richiesta.

Sicurezza fisica

Le server room e i datacenter devono essere ad accesso controllato e provvisti di misure di sicurezza fisica (antincendio, antiallagamento, controllo della temperatura, continuità elettrica).

Sviluppo di software sicuro

Lo sviluppo sicuro deve avvenire secondo i principi di privacy-by design e security-by-design. In particolare, gli ambienti di test devono essere separati dagli ambienti di produzione e non devono utilizzare dati reali.

Autenticazione forte

Deve essere implementato un sistema di autenticazione a 2 fattori per accessi degli amministratori di sistema e per tutti gli accessi a sistemi utilizzati per il trattamento di dati genetici o qualificati come "a maggior tutela".

ALLEGATO 2

MISURE DI SICUREZZA ORGANIZZATIVE RELATIVE AI DATI PERSONALI - FACSIMILE

2. MISURE DI SICUREZZA ORGANIZZATIVE

Nella tabella di seguito riportata sono indicate le misure di sicurezza organizzative relative ai dati personali previste da IIT ai sensi del Regolamento Generale sulla protezione dei dati personali n. 679/2016 e s.m.i. (di seguito "GDPR"), per cui si richiede a XXX la dimostrazione della conformità attraverso la compilazione della colonna "Compliance Status Partner".

Nel caso in cui XXX non sia in grado di soddisfare in tutto o in parte i requisiti richiesti, è tenuto a specificarne la motivazione nella colonna "Note giustificative".

2.1. Misure di sicurezza organizzative

Item #	**Categoria**	**Controllo**	**Compliance status IIT** (S/N/n.a.)	**Compliance status Parte XXX** (S/N/n.a.)	**Note giustificative** (se non applicabile, non implementato o parzialmente implementato, darne motivazione indicando i controlli compensativi applicati in sostituzione)
1	Analisi dei rischi	È stata effettuata l'analisi dei rischi e sono stati definiti ed implementati gli action plan per l'adeguamento delle misure di sicurezza organizzative (laddove necessario). L'analisi dei rischi viene costantemente aggiornata.			
2	Attribuzione di funzioni e compiti a soggetti autorizzati	Il personale interno che tratta dati personali è designato con apposito atto di nomina.			

3	Istruzioni al personale interno autorizzato al trattamento dei dati personali	Comunicazione di apposite istruzioni scritte al personale interno autorizzato al trattamento dei dati personali.			
4	Canale dedicato per la notifica delle violazioni di Dati Personali (se applicabile)	È disponibile un apposito canale per la comunicazione delle eventuali violazioni degli obblighi in tema di trattamento di Dati Personali.			
5	Designazione del Responsabile della Protezione dei Dati (se applicabile)	È designato un Responsabile della Protezione dei Dati a cui è affidato il compito di valutare ed organizzare la gestione del trattamento dei dati personali.			
6	Pseudonimizzazione dei dati personali (laddove applicabile):	Applicazione di misure di de-identificazione dei dati personali, in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive. Le informazioni aggiuntive sono conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.			

2.2. Referente GDPR di XXX verso IIT

Per informazioni sulla checklist dei controlli di sicurezza organizzativi, IIT può fare riferimento a:

Nome, Cognome .....
Indirizzo e-mail .....
Contatto telefonico .....

2.3. Referente GDPR di IIT verso XXX

Per informazioni sulla checklist dei controlli di sicurezza organizzativi, XXX può fare riferimento a:

GDPR Team
gdpr@iit.it
+39 010 28961