**CONTRATTO PER LA DESIGNAZIONE DEL RESPONSABILE**
**DEL TRATTAMENTO DI DATI PERSONALI**

20 SETTEMBRE 2022

L'ISTITUTO NAZIONALE DI FISICA NUCLEARE (di seguito INFN) con sede legale in via E. Fermi, 54 Frascati (Roma), Codice Fiscale: 84001850589 (**TITOLARE DEL TRATTAMENTO**), in persona del suo Presidente p.t.[1] / rappresentato per tale atto dal Direttore p.t. di ....., in forza della deliberazione del Consiglio Direttivo dell'INFN n. 14844 del 27 luglio 2018[2]

e

…….. (di seguito Operatore Economico) con sede legale ……. Codice Fiscale: ……., in persona del legale rappresentante o persona appositamente autorizzata giusta delega (**RESPONSABILE DEL TRATTAMENTO**),

**premesso che**

il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito anche Regolamento) dispone che il soggetto che effettui un trattamento dei dati personali per conto del titolare è individuato responsabile del trattamento e vincolato a una condotta conforme ai principi indicati nel Regolamento nonché all'adozione di misure tecniche e organizzative adeguate per un'efficace protezione dei dati personali;
l'INFN, con deliberazione del Consiglio Direttivo n. 14844 del 27 luglio 2018, ha individuato il proprio assetto organizzativo in materia di trattamento dei dati personali assegnando ai Direttori delle Strutture in cui si l'Istituto si articola, tra gli altri, il compito di designare quali Responsabili del trattamento i soggetti che trattano dati personali per conto dell'INFN nell'ambito dei contratti o delle convenzioni che hanno il potere di sottoscrivere;
con atto n. …… del ……. la Giunta Esecutiva / il Direttore di …… ha affidato a ……. l'appalto per ……;
le attività affidate comportano il trattamento di dati personali per conto dell'INFN;
l'INFN è titolare del trattamento dei dati personali coinvolti nelle attività di cui ai precedenti capoversi e in quanto tale determina le finalità e i mezzi del loro trattamento;
l'INFN attribuisce assoluto interesse a che i dati personali dei quali è titolare siano trattati secondo i più elevati standard di tutela, anche nell'espletamento delle attività oggetto di appalto;
l'INFN intende consentire all'Operatore Economico l'accesso al trattamento dei dati personali di cui è titolare nel ristretto limite in cui il loro trattamento è necessario ad adempiere ai compiti oggetto dell'attività affidata;
l'INFN ha preso atto delle dichiarazioni secondo le quali il responsabile si impegna a mettere in atto misure tecniche ed organizzative adeguate ad assicurare che il trattamento dei dati personali

1 Per gli atti approvati dalla Giunta Esecutiva.

2 Per gli atti di competenze delle Strutture.

effettuato per conto del titolare soddisfi i requisiti del Regolamento UE 2016/679, nel seguito anche Regolamento, e garantisca la tutela degli interessati;

**le Parti in epigrafe individuate e rappresentate convengono e stipulano quanto segue.**

1. Le premesse formano parte integrante e sostanziale del presente contratto.

2. Il titolare, ai sensi dell'articolo 28 del Regolamento, designa l'Operatore Economico quale responsabile del trattamento dei dati personali trattati per suo conto e autorizza le operazioni di trattamento necessarie per eseguire le attività previste nel contratto/ordine nelle premesse indicato e nei limiti delle finalità ivi specificate e descritte in dettaglio nell'**Allegato A.**

3. Per la durata del contratto / ordine, il responsabile del trattamento dei dati personali designato, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia di dati personali trattati, delle categorie di interessati nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, si impegna nei confronti del titolare a:

trattare i dati personali nel rispetto dei princìpi e delle disposizioni previsti dal Codice, dal Regolamento, dagli indirizzi e dai provvedimenti a carattere generale emanati dal Garante in materia di protezione dei dati personali e da ogni altra vigente normativa in materia di protezione dei dati personali, nonché delle istruzioni fornite nel presente atto;
garantire e vigilare che i propri dipendenti e/o le persone autorizzate al trattamento dei dati personali:
si siano impegnate a effettuare il trattamento dei dati personali oggetto del contratto / ordine, nel rispetto delle disposizioni di cui al precedente capoverso e alla riservatezza o, se del caso, abbiano un adeguato obbligo legale di riservatezza;
ricevano formazione periodica relativa alla sicurezza dei dati e alla privacy;
abbiano ricevuto le istruzioni idonee alle attività da svolgere, finalizzate a trattare in modo sicuro e riservato i dati affidati, custodendoli e controllandoli nel modo più appropriato e sicuro;
concedere l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto;
designare, ove richiesto in base al Regolamento, un responsabile della protezione dei dati, in conformità a quanto disposto dall'art. 37 e ss. del Regolamento e comunicare i dati di contatto all'Autorità di controllo e al titolare del trattamento;
tenere il registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare ai sensi dell'art. 30, comma 2 del Regolamento, e, su richiesta, metterlo a disposizione del titolare e/o dell'Autorità di controllo;
mettere in atto almeno le misure tecniche e organizzative specificate nell'**ALLEGATO B SMALL | MEDIUM | LARGE**[3] per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati;
nei casi in cui evidenzi una non piena corrispondenza tra la tipologia di trattamento prevista dal contratto / ordine e le misure di sicurezza richieste, impegnarsi a comunicarlo per scritto al titolare, fornendogli l'analisi del rischio effettuata e indicando le misure di sicurezza che ritiene adeguate;

3 La scelta del modello è legata alla complessità del trattamento, alla quantità di dati personali trattati e alla loro tipologia (comuni, particolari, genetici, ecc. ecc.).

implementare le ulteriori misure di sicurezza che il titolare può chiedere nel caso in cui il trattamento, per la propria natura, il contesto e/o le tecnologie utilizzate, ne evidenzi la necessità;
collaborare con il titolare — nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse — affinché siano sviluppate, adottate e implementate misure correttive di adeguamento a nuovi requisiti previsti da qualsivoglia modifica della normativa in materia di trattamento dei dati personali intervenuta durante l'esecuzione del contratto / ordine che generi nuovi requisiti, ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali;
assistere il titolare nel garantire il rispetto degli obblighi concernenti la sicurezza dei dati personali (in particolare: sicurezza del trattamento, notifica della violazione dei dati personali all'Autorità di controllo e relativa comunicazione all'interessato), la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva con l'Autorità di controllo, ai sensi degli articoli da 32 a 36 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile;
comunicare al titolare presso l'indirizzo PEC ……[4] qualsiasi elemento che possa compromettere il corretto trattamento dei dati personali e, senza ritardo e per iscritto, ogni violazione dei dati personali; in particolare, il responsabile garantirà il rispetto delle prescrizioni di cui all'art. 33 del Regolamento e fornirà al titolare una descrizione dettagliata utilizzando il modello di notifica interna di violazione dati personali, disponibile all'indirizzo: https://dpo.infn.it/documenti-dpo/violazione-dati-personali-e-relativi-modelli/;
informare immediatamente il titolare qualora, a suo parere, un'istruzione dallo stesso fornita violi il Regolamento o altre norme applicabili in materia di protezione dei dati;
assistere il titolare nell'adempimento dei propri obblighi derivanti dall'esercizio, da parte degli interessati, dei diritti di cui alla Sezione 3 del Regolamento, inoltrando tempestivamente, e comunque nel più breve tempo possibile, le istanze al titolare e supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti;
non ricorrere a un altro responsabile senza la previa autorizzazione scritta del titolare;
ogniqualvolta il titolare autorizzi il ricorso del responsabile ad altro responsabile per l'esecuzione di specifiche attività, il responsabile designato con il presente atto impone a tale altro responsabile, mediante la stipula di un contratto o altro atto giuridico, i medesimi obblighi in materia di protezione dei dati personali contenuti nella presente designazione; una copia di tale accordo di Sub-responsabile e le successive modifiche deve — su richiesta del titolare — essere presentata al titolare, dando così al titolare la possibilità di garantire che gli stessi obblighi di protezione dei dati stabiliti nelle clausole sono imposti al sub-responsabile; se il sub-responsabile non adempie ai propri obblighi in materia di protezione dei dati, il responsabile resta pienamente responsabile nei confronti del titolare per quanto riguarda l'adempimento degli obblighi del sub-responsabile;
adottare eventuali procedure di conservazione dei dati e delle informazioni nella propria disponibilità, per un periodo di tempo non superiore a quello strettamente necessario per adempiere agli obblighi di legge o per perseguire le finalità per le quali sono stati raccolti dallo stesso titolare o successivamente utilizzati;
non trasferire, né in tutto né in parte, in un Paese terzo o a un'organizzazione internazionale i dati personali trattati ai sensi del Contratto, senza la previa autorizzazione del titolare;
nel trattare i dati personali per conto del titolare, attenersi alle istruzioni da questo fornite, anche in caso di eventuale trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o la normativa nazionale; in tal caso, il responsabile si impegna a informare il titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

4 PEC dell'AC per contratti approvati da GE e PEC della Struttura per quelli di competenza dei Direttori.

mettere a disposizione del titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui alla presente designazione e di cui all'art. 28 del Regolamento nonché consentire e contribuire alle attività di revisione, comprese le ispezioni, eseguite dal titolare o da altro soggetto da questi incaricato;
avvisare tempestivamente e senza ingiustificato ritardo il titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità di controllo; inoltre, deve assistere il titolare nel caso di richieste formulate dall'Autorità di controllo in merito al trattamento dei dati personali effettuate in ragione del contratto;
a scelta e su richiesta del titolare, cancellare o restituire al medesimo tutti i dati personali al termine del contratto/ordine o comunque della prestazione dei servizi relativi al trattamento, nonché cancellare le copie esistenti documentando per iscritto l'adempimento di tale operazione, salvo che il diritto dell'Unione o la normativa nazionale prevedano la conservazione dei dati.

4. In conformità a quanto disposto dall'art. 28, comma 10 del Regolamento, nel caso in cui il responsabile violi gli obblighi per la stessa previsti dal Regolamento e ad esso attribuiti dal presente contratto, determinando le finalità ed i mezzi del trattamento, esso sarà considerato ai fini sanzionatori, titolare del trattamento effettuato.

5. Il titolare si riserva di effettuare, anche tramite soggetti terzi appositamente autorizzati e previo congruo preavviso, verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali da parte del responsabile e dei suoi eventuali Sub-responsabili. Nel caso in cui all'esito di tali verifiche le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che l'Operatore Economico agisca in modo difforme o contrario alle istruzioni fornite dal titolare, quest'ultimo darà un termine congruo per adeguarsi, applicando le penali previste per l'eventuale ritardo. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 c.c., il titolare, in ragione della gravità o del perdurante dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

6. Il responsabile del trattamento risponde dei danni derivati dal trattamento qualora non abbia adempiuto agli obblighi della normativa vigente in materia di trattamento dei dati personali o abbia agito in modo difforme alle istruzioni fornite dal titolare.

7. Il presente contratto non comporta alcun diritto del responsabile a compensi o rimborsi aggiuntivi rispetto quelli già previsti nel contratto principale cui il presente accordo accede.

8. Per quanto non espressamente previsto nel presente atto, si fa espresso riferimento alla normativa, sia europea sia nazionale, in materia di protezione dei dati personali.

9. Le clausole del presente contratto si applicano per tutta la durata del contratto / ordine per il quale è stato stipulato. Le clausole possono essere modificate d'intesa fra e parti se cambiano le condizioni del trattamento previsto nel contratto principale e finché quest'ultimo resta vigente il presente contratto non può essere autonomamente risolto se non sostituito con un altro contratto che disciplini il trattamento dei dati.

Luogo e data …….....

Per il titolare del trattamento

Per il responsabile del trattamento

# ALLEGATO A

## DESCRIZIONE DEL TRATTAMENTO

### CATEGORIE DI INTERESSATI I CUI DATI PERSONALI SONO TRATTATI

.....

.....

### CATEGORIE DI DATI PERSONALI TRATTATI

.....

.....

### EVENTUALI DATI PARTICOLARI TRATTATI E LIMITAZIONI O GARANZIE APPLICATE[5]

.....

.....

### NATURA DEL TRATTAMENTO

.....

.....

### FINALITÀ PER LE QUALI I DATI PERSONALI SONO TRATTATI PER CONTO DEL TITOLARE

.....

.....

### DURATA DEL TRATTAMENTO

.....

.....

5 Devono tenere conto della natura dei dati e dei rischi connessi, p.e. una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

# ALLEGATO B (SMALL)

## MISURE TECNICHE E ORGANIZZATIVE,

## COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

Ogni Incaricato al trattamento deve possedere delle credenziali di autenticazione, hardware o software, a suo uso esclusivo, di elevata robustezza.
Devono essere prescritte le cautele necessarie per assicurare la segretezza della componente riservata delle credenziali e/o la diligente custodia del dispositivo in possesso e uso esclusivo dell'Incaricato.
Le credenziali di autenticazione sono personali e non devono essere assegnate ad altri, neppure in tempi diversi.
Le credenziali di accesso devono essere disabilitate quando cessi la necessità di accesso o in caso di inattività superiore a sei mesi. Devono essere predisposte delle procedure per assicurare la disponibilità di dati o strumenti in caso di prolungata assenza o impedimento dell'Incaricato.
La sussistenza delle ragioni che hanno portato al rilascio delle autorizzazioni agli Incaricati deve essere verificata con periodicità almeno annuale. Le utenze amministrative devono essere utilizzate solamente quando indispensabili, registrando ogni accesso effettuato.
Assicurare la totale distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
Le utenze amministrative generiche, quali "root" di UNIX o "Administrator" di Windows, devono essere impiegate solo per le situazioni di emergenza e in modo da assicurare l'imputabilità di chi ne fa uso.
Deve essere redatto e mantenuto aggiornato un elenco con gli estremi identificativi delle persone fisiche con accesso privilegiato e con la descrizione delle funzioni che sono state loro attribuite nell'ambito delle attività svolte per conto del titolare; per quelle che rivestono il ruolo di Amministratori di Sistema, devono essere implementate le ulteriori misure di sicurezza, come definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27/11/2008 *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema* e s.m.i..
Limitare l'accesso ai dati personali nei file system, nelle condivisioni di rete, applicazioni e database, utilizzando *access control list* nei sistemi, solo a persone con esigenze valide.
Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
Devono essere utilizzati e mantenuti aggiornati idonei programmi contro il rischio di esecuzione di malware, di intrusione e accesso abusivo.
Disattivare l'esecuzione automatica dei contenuti dinamici (p.e. macro) presenti nei file
Disattivare l'apertura automatica dei messaggi di posta elettronica.
Disattivare l'anteprima automatica dei contenuti dei file.
Configurare i blocca schermo per limitare l'accesso a workstation in cui viene eseguito il trattamento dei dati personali.
Disconnettere automaticamente gli utenti dalle applicazioni in esecuzione sui sistemi su cui viene eseguito il trattamento di dati personali, dopo un periodo definito di inattività.
Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.
Mantenere aggiornati il sistema operativo e le applicazioni.

Ogni volta che vi sia la segnalazione della presenza di vulnerabilità nei sistemi utilizzati, si deve provvedere con sollecitudine al loro aggiornamento.
Tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature devono essere eseguite solo utilizzando connessioni protette.
Devono essere utilizzati, almeno settimanalmente, e periodicamente verificati, sistemi di salvataggio e ripristino dei dati: quest'ultimo deve avere tempi certi e comunque non superiori a sette giorni.
Assicurare la riservatezza delle informazioni contenute nelle copie di salvataggio, mediante adeguata protezione fisica dei supporti o cifratura, avendo cura che almeno una di esse non sia permanentemente accessibile dal sistema, per evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di salvataggio. La cifratura effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
Registrare le eventuali operazioni di ripristino dei dati, includendo il nominativo della persona responsabile, la descrizione dei dati ripristinati e il motivo per cui il ripristino si è reso necessario
Il trasferimento di dati deve sempre avvenire utilizzando connessioni cifrate.

# ALLEGATO B (MEDIUM)

## MISURE TECNICHE E ORGANIZZATIVE,

## COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

Misure di SMALL.

Nel caso di trattamento di dati particolari, come definiti dall'Art. 9 del Regolamento, il responsabile deve assicurare che la loro memorizzazione avvenga in maniera da non permettere la diretta identificazione dell'interessato, p.e. cifrandoli o mantenendoli separati dagli altri dati personali.
Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
Predisporre documenti sulla sicurezza in cui vengono descritte le misure di protezione adottate e le relative procedure

Definire un piano di gestione dei rischi, documentandoli e gestendoli di conseguenza, che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati. Il piano deve essere rivisto periodicamente.

Eseguire, regolarmente e ad ogni variazione significativa di configurazione, scansioni sui propri sistemi, alla ricerca di software non autorizzato e vulnerabilità, avendo cura di mantenere sempre aggiornati gli strumenti utilizzati.

Verificare che le vulnerabilità emerse dalle scansioni siano state risolte, per mezzo di patch, o implementando opportune contromisure o documentando e accettando un ragionevole rischio
Adottare e implementare un processo di gestione degli incidenti di sicurezza per assicurare un'immediata comunicazione, analisi d'impatto e efficaci azioni correttive e preventive.

# ALLEGATO B (LARGE)

## MISURE TECNICHE E ORGANIZZATIVE,

## COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

Misure di MEDIUM

Se viene sviluppato software, seguire le *Linee guida per lo sviluppo del software sicuro* pubblicate dall'Agenzia per l'Italia Digitale.

Implementare e mantenere aggiornato un inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP;

Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.

Definire ed impiegare configurazioni sicure standard per workstation, server e altri tipi di sistemi usati dall'organizzazione, memorizzando le immagini di installazione offline.

Eventuali sistemi compromessi devono essere ripristinati utilizzando la configurazione standard.

Monitorare i sistemi su cui viene eseguito il trattamento di dati personali, per la creazione di utenti amministratori non autorizzati o l'assegnazione non autorizzata di privilegi a un utente esistente.

Copiare i log di sistema e degli eventi dai sistemi su cui viene eseguito il trattamento su di un sistema al di fuori del controllo dell'amministratore di sistema o dell'operatore le cui attività vengono registrate.

Utilizzare gli strumenti di monitoraggio dei log al fine di rilevare comportamenti dannosi o possibili violazioni del sistema.

Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.

Installare su tutti i dispositivi *firewall* ed IPS personali.

Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.

Filtrare il contenuto del traffico web.

Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (p.e.. .cab)

Bloccare il traffico da e verso URL presenti in una *blacklist*.

Verificare le regole dei *firewall* e degli altri dispositivi di filtraggio con periodicità almeno annuale. Documentare le eventuali variazioni.

Limitare l'accesso alle strutture in cui sono situati i sistemi informativi che elaborano i dati a individui identificati e autorizzati.

Nominare uno o più funzionari addetti alla sicurezza, responsabili del coordinamento e del monitoraggio delle regole e delle procedure di sicurezza.