CONTRATTO PER LA DESIGNAZIONE DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI.

28 FEBBRAIO 2019

L'ISTITUTO NAZIONALE DI FISICA NUCLEARE (di seguito anche INFN) con sede legale in via E. Fermi, 40 Frascati (Roma), Codice Fiscale: 84001850589, in persona del Presidente pro-tempore/del Direttore …… della Struttura INFN di ……..]

TITOLARE DEL TRATTAMENTO

e

L'operatore economico/ altro soggetto in caso di Convenzioni ……. con sede ……. Codice Fiscale: ……., in persona del legale rappresentante/persona appositamente autorizzata giusta delega …….

RESPONSABILE DEL TRATTAMENTO

congiuntamente definite anche Parti,

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 una efficace protezione dei dati personali;
- con deliberazione/ordine n. …… del …… la Giunta Esecutiva/il Direttore della Struttura INFN …… ha affidato all'operatore economico [altro soggetto in caso di Convenzioni] ……. il servizio [l'attività] di ……;

- le attività oggetto del servizio affidato comportano il trattamento di dati personali;
- l'INFN è Titolare del trattamento dei dati personali coinvolti nelle prestazioni oggetto del servizio/convenzione 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 del servizio oggetto di appalto/convenzione;
- 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;
- l'INFN intende consentire all'operatore economico/altro soggetto …….. 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 del servizio affidato/della convenzione stipulata;
- l'INFN ha preso atto delle dichiarazioni secondo le quali l'operatore economico/altro soggetto garantisce di mettere in atto misure tecniche ed organizzative adeguate per assicurare che il trattamento dei dati personali effettuato per conto dell'INFN soddisfi i requisiti del Regolamento UE 2016/679 e garantisca la tutela degli interessati;

tutto quanto sin qui premesso, le Parti in epigrafe individuate e rappresentate

convengono e stipulano quanto segue.

1. Le premesse formano parte integrante e sostanziale del presente contratto.
2. L'INFN individua l'operatore economico/altro soggetto …….. Responsabile del trattamento dei dati personali trattati per suo conto e affida allo stesso le operazioni di trattamento necessarie per eseguire il contratto/la convenzione stipulata.
3. Per la durata del contratto/convenzione e per le attività in esso disciplinate, 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:
    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;
    b. 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;

c. 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;

d. 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;

e. nel trattare i dati personali per conto del Titolare, attenersi alle istruzioni fornite dal Titolare stesso, 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 del trattamento 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;

f. osservare quale livello minimo di sicurezza, le prescrizioni previste dal Contratto e dagli eventuali suoi allegati, adottando misure non inferiori alle *"Norme per il trattamento dei dati personali nell'INFN"* disponibili all'indirizzo web https://dpo.infn.it/ oltre, ove applicabili, le *"Linee guida per lo sviluppo del software sicuro"* pubblicate dall'Agenzia per l'Italia Digitale e ogni altra eventuale comunicazione scritta del Titolare concernente le modalità di trattamento dei dati da parte del Responsabile;

g. adottare, nei trattamenti effettuati con strumenti informatici misure non inferiori alle seguenti:

   - garantire che ogni incaricato possieda una credenziale personale di autenticazione a suo uso esclusivo (p.e. username / password o un dispositivo hardware di autenticazione);
   - prescrivere le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso e uso esclusivo dell'Incaricato;
   - verificare che l'eventuale password sia composta da almeno dieci caratteri alfanumerici, che non contenga riferimenti facilmente riconducibili all'incaricato, che venga modificata da quest'ultimo al primo utilizzo e, successivamente, con ragionevole frequenza;
   - garantire che l'eventuale codice identificativo personale, non sia assegnato ad altri incaricati, neppure in tempi diversi;
   - eliminare il codice identificativo personale quando cessi la necessità di accesso da parte dell'incaricato e disabilitarlo nel caso di inattività superiore a sei mesi;
   - predisporre le procedure per assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato;
   - limitare al minimo indispensabile i privilegi di autorizzazione di ogni singolo incaricato o gruppo omogeneo;
   - verificare, con periodicità almeno annuale, la sussistenza delle ragioni che hanno portato al rilascio delle autorizzazioni;

- redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del Titolare e implementare 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.;
- utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato e assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse;
- utilizzare le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, solo per le situazioni di emergenza, gestendo le credenziali relative in modo da assicurare l'imputabilità di chi ne fa uso
- utilizzare e mantenere aggiornati idonei programmi contro il rischio di esecuzione di malware, di intrusione e accesso abusivo;
- eseguire regolarmente scansioni sui propri sistemi alla ricerca di software non autorizzato e vulnerabilità, avendo cura di mantenere sempre aggiornati gli strumenti utilizzati;
- eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature solo tramite connessioni protette;
- ogni volta che vi sia la segnalazione della presenza di vulnerabilità nei sistemi utilizzati, provvedere con sollecitudine al loro aggiornamento;
- definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati;
- utilizzare, e verificare periodicamente, 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 sicurezza;

inoltre, per il 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;
- assicurare che il loro trasferimento in formato elettronico avvenga in maniera cifrata;

h. implementare, sia nei trattamenti effettuati in modo informatico sia cartaceo, le misure tecniche e organizzative di sicurezza impartite dal Titolare al fine di assicurare, in ragione del proprio assetto organizzativo, ogni più efficace livello di sicurezza dei dati personali trattati per conto del Titolare; il Responsabile deve informare il Titolare qualora ritenga che un'istruzione impartitagli da quest'ultimo violi il Regolamento o altre disposizioni europee o nazionali relative alla protezione dei dati;

i. assistere il Titolare nell'adempimento dei propri obblighi derivanti dall'esercizio, da parte degli interessati, dei diritti di cui alla Sezione 3 del Regolamento e individuare, di concerto con il Titolare, una procedura idonea a fornire sollecita risposta all'interessato nel caso in cui questi formuli istanza di accesso ai dati trattati per conto del Titolare, nonché per l'esercizio di tutti i diritti che la legislazione europea e nazionale pone a sua tutela;

j. adottare tutte le misure di sicurezza di cui all'art. 32 del Regolamento; nel caso in cui il trattamento, per la propria natura, il contesto e/o le tecnologie utilizzate, necessiti di una valutazione d'impatto sulla protezione dei dati e/o evidenzi la necessità di approntare ulteriori misure di sicurezza, il Titolare può chiedere al Responsabile la loro implementazione; il Responsabile, nei casi in cui evidenzi una non piena corrispondenza tra la tipologia di trattamento prevista dal contratto/dalla convenzione e le misure di sicurezza richieste, si impegna a comunicarlo per scritto al Titolare, fornendogli l'analisi del rischio effettuata e indicando le misure di sicurezza che ritiene adeguate;

k. 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 al Garante per la protezione dei dati personali e relativa comunicazione all'interessato), la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva con il Garante, 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 qualsiasi elemento che possa compromettere il corretto trattamento dei dati personali e, senza ritardo e per iscritto, comunicare 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: i) della violazione verificatasi, ii) dei dati personali interessati (comprensivi delle categorie e del numero approssimativo degli interessati), iii) delle categorie e del numero approssimativo delle registrazioni dei dati personali interessati, iv) delle probabili conseguenze della violazione, v) nonché ogni ulteriore informazione e/o documentazione richiesta dal Titolare, non appena disponibili; 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.

l. 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 di trattamento, 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; il Responsabile designato con il presente atto accerta la sussistenza, in capo al Responsabile dal medesimo

designato, delle garanzie sufficienti alla messa in atto delle misure tecniche e organizzative adeguate richieste dal Regolamento e conserva, nei confronti del Titolare del trattamento anche in caso di inadempimento dell'altro Responsabile, l'intera responsabilità dell'adempimento di tali obblighi;

m. garantire e vigilare che i propri dipendenti e/o le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, che 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 e, in ogni caso, che abbiano ricevuto la formazione necessaria;

n. tenere il registro delle categorie di attività relative al trattamento dei dati personali effettuate per conto del Titolare ai sensi dell'art. 30, comma 2 del Regolamento, e, su richiesta, mettere tale registro a disposizione del Titolare e/o del Garante per la protezione dei dati personali;

o. 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;

p. a scelta e su richiesta del Titolare, cancellare o restituire al medesimo tutti i dati personali al termine del Contratto o comunque della prestazione dei servizi relativi al trattamento nonché cancellare le copie esistenti, 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 ed 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 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.
6. 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.

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

Luogo e data .....

Per l'operatore economico/altro soggetto	Per l'INFN
Responsabile del trattamento	Titolare del trattamento
Il legale rappresentante	Il Presidente/Direttore