GUIDA ALLA COMPILAZIONE DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Versione 1.0

30/10/2025

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

SOMMARIO

INTRODUZIONE

Cos'è il registro delle attività di trattamento dei dati personali (RAT)

L'articolo 30 del GPDR prevede tra gli adempimenti principali del titolare e del responsabile del trattamento dei dati personali la tenuta del registro delle attività di trattamento dei dati personali (di seguito "RAT").

- Il RAT è un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GPDR) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.
- Il RAT costituisce uno dei principali elementi di *accountability* del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.
- Il RAT deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.
- Il RAT si compone di singole schede, ciascuna riferita ad un solo trattamento.
- Il RAT deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere: ogni nuovo trattamento in precedenza non previsto dovrà avere una nuova scheda; le modifiche ai trattamenti in essere dovranno comportare l'aggiornamento della relativa scheda; la cessazione dei trattamenti in essere determineranno la cancellazione della scheda inserita nel registro.

Chi compila il RAT?

Secondo quanto indicato al punto n. 5 della delibera INFN N. 14844 del Consiglio Direttivo del 27/07/2018: *"I soggetti individuati nel capoverso 3[1] hanno il compito di provvedere alla effettiva e concreta attuazione delle misure tecniche ed organizzative volte a garantire e dimostrare che il trattamento dei dati personali è effettuato conformemente al Regolamento presso ciascuna Struttura, articolazione o ufficio che dirigono o di cui hanno la responsabilità. In particolare: [...]*

d) implementano il Registro del trattamento dei dati personali, comunicando al DPO i nuovi trattamenti in uso presso la Struttura o l'articolazione che dirigono o di cui hanno la responsabilità".

È quindi compito dei Direttori delle varie strutture INFN implementare il RAT. Per assolvere a tale compito il Direttore dovrà avvalersi dei Responsabili delle articolazioni interne ciascuna Struttura i quali verificheranno le attività di propria competenza che coinvolgono il trattamento di dati personali.

[1] *"[...] i Direttori delle Strutture [...]"*

PIATTAFORMA PER LA COMPILAZIONE

Per semplificare la gestione del RAT e la sua compilazione nel rispetto di quanto previsto dall'articolo 30 del GDPR, su iniziativa del DPO attraverso il Sistema Informativo, è stata realizzata una piattaforma web.

Per utilizzare la piattaforma:

- collegarsi con un browser web all'indirizzo:
  https://ratp.dsi.infn.it
- autenticarsi con INFN-AAI.

L'accesso alla piattaforma è consentito ai seguenti soggetti:

- L'operatore/inseritore (USER) è chi, in un servizio/ufficio, compila effettivamente il trattamento, facendosi aiutare se necessario dal referente privacy;
- Il Responsabile (RESP) di quel servizio/ufficio FIRMA/ARCHIVIA;
- Il Direttore di Struttura (HEAD) VISTA/RESPINGE i trattamenti di tutti i servizi/uffici.

Stati di un trattamento

I ruoli consentono le seguenti modifiche di stato di un trattamento:

- IN_BOZZA: creazione nuovo trattamento - **User**
- SOTTOMESSO: sottomesso trattamento per la firma, se stato precedente IN_BOZZA o RESPINTO - **User**
- FIRMATO: se stato precedente SOTTOMESSO - **Resp**
- RESPINTO: se stato precedente FIRMATO - **Head**
- VISTATO: se stato precedente FIRMATO - **Head**
- ARCHIVIATO: se stato precedente VISTATO - il trattamento è congelato (no nuove versioni) - **Resp**
- SUPERATO: viene VISTATA una nuova versione dello stesso trattamento (automatico)

Note:

- Un trattamento può essere modificato solo se in stato IN_BOZZA.
- Si può creare una nuova versione di un trattamento solo se in stato VISTATO; quando la nuova versione viene vistata, la precedente transita automaticamente nello stato SUPERATO.
- Un trattamento in stato VISTATO/ARCHIVIATO/SUPERATO non può essere eliminato (rimane nello storico), in tutti gli altri casi il trattamento può essere eliminato definitivamente: dall'utente **User** se in stato IN_BOZZA/SOTTOMESSO/RESPINTO o dall'utente **Resp** se FIRMATO.

Come individuare un trattamento?

Prima di iniziare a compilare uno specifico trattamento devono essere fatte alcune considerazioni al fine di identificare correttamente ogni singolo trattamento che sarà interessato da una singola scheda.

Sarà opportuno verificare anche che l'elenco dei trattamenti sia consistente con l'elenco delle attività che spesso vengono riportate nei siti web di Sede per ogni servizio.

Un trattamento non è un'attività isolata ma un insieme di operazioni che hanno lo stesso scopo e coinvolgono i medesimi dati.

Questi i passaggi che devono esser presi in considerazione per individuare uno specifico trattamento:

1. **individuare** le attività di competenza della Struttura che coinvolgono dati personali;
2. **identificare** i dati personali raccolti, le modalità di raccolta e lo scopo;
3. **analizzare** il percorso dei dati dall'acquisizione alla conservazione, uso, e infine alla cancellazione;
4. **raggruppare** le attività sulla base delle loro finalità, lo scopo cioè per cui i dati vengono trattati. Attività diverse, anche se usano gli stessi dati, possono costituire trattamenti separati se hanno finalità distinte. Ad esempio: l'uso dei dati dei dipendenti per la gestione delle paghe è un trattamento; l'uso degli stessi dati per la formazione interna è un altro trattamento, perché ha una finalità diversa;
5. una volta identificato il trattamento, **raccogliere** tutte le informazioni necessarie per la sua descrizione nell'apposita scheda del registro.

Nel seguito della presente guida viene descritto il processo di compilazione di una scheda del Registro riferita ad un particolare trattamento.

COMPILAZIONE DELLA SCHEDA DI TRATTAMENTO

Per aggiungere un nuovo trattamento, dopo essersi autenticati nella piattaforma:

- fare click su "*Template*s" in alto a destra della pagina,
- nella Lista template andare sulla riga "Template TRATTAMENTO" e fare click sull'icona Azioni "**Crea un nuovo trattamento**";
- quindi riempire i campi come descritti nel seguito.

Informazioni generali

Nome del trattamento	Inserire un titolo identificativo del trattamento (ad es. gestione concorsi, gestione newsletters, videosorveglianza, etc.). Nella tabella riepilogativa dei trattamenti il trattamento sarà identificato dal **Nome** scelto e sulla base di questo sarà possibile effettuarne la ricerca.
Sede INFN	Inserire la Sede INFN presso la quale viene effettuato il trattamento. Nella tabella riepilogativa dei trattamenti per ogni trattamento viene riportata la **Sede INFN** di riferimento e sulla base di questa sarà possibile effettuarne la ricerca.
Servizio	Inserire la denominazione dell'articolazione interna la Struttura presso il quale viene effettuato il trattamento (per esempio "Servizio di Direzione", "Servizio Calcolo e Reti", "Ufficio Missioni", etc.). Nella tabella riepilogativa dei trattamenti per ogni trattamento viene riportato il **Servizio** di riferimento e attraverso questo sarà possibile effettuare la relativa ricerca.

Trattamento

Descrizione sintetica del trattamento	Descrivere il trattamento con poche parole chiave. Ad es: conferimento e gestione degli incarichi di associazione.
Data di compilazione	Data in cui viene compilato il trattamento.
Finalità del trattamento	Descrivere una o più finalità del trattamento (max 500 caratteri). Nel GDPR, all'articolo 5, paragrafo 1, lettera b) - Principi applicabili al trattamento dei dati personali, è riportato: i dati *"devono essere raccolti per finalità determinate, esplicite e legittime e non devono essere successivamente trattati in modo incompatibile con tali finalità"*. Ad es: vedi l'informativa INFN relativa agli eventi[2].
Titolare del trattamento	Il titolare dei trattamenti posti in essere dall'INFN è l'INFN. Vedi la sezione «Definizioni» di questo documento.

[2]https://dpo.infn.it/documenti-dpo/informative-e-modelli-personalizzabili/

Responsabile del trattamento	Se presente, inserire i riferimenti (nome e dati di contatto) del Responsabile del trattamento. Vedi la sezione «Definizioni» di questo documento.
SUB-responsabile/i del trattamento	Se presente/i inserire il/i riferimenti (nome e dati di contatto) di SUB-responsabile/i del trattamento. Vedi la sezione «Definizioni» di questo documento.
Cotitolare	Se presente/i inserire il o i riferimenti (nome e dati di contatto) di Cotitolari. Vedi la sezione «Definizioni» di questo documento.
Quando e in quale forma viene rilasciata l'Informativa relativa a questo trattamento?	L'informativa deve esser resa prima dell'inizio del trattamento nelle forme e modi che devono essere descritti nel presente punto. Modelli standard di Informativa da adattare ai particolari trattamenti sono reperibili in: https://dpo.infn.it/documenti-dpo/informative-e-modelli-personalizzabili/ ed in https://www.ac.infn.it/informative_privacy.html
Base giuridica	Selezionare una o più voci della lista: CONSENSO (*se l'interessato ha acconsentito al trattamento*); CONTRATTO (*se il trattamento è necessario per la stipula o l'esecuzione di un contratto tra il titolare e l'interessato*); OBBLIGO LEGALE (*se il trattamento è necessario per adempiere ad un obbligo legale al quale l'INFN è soggetto*); SALVAGUARDIA INTERESSI VITALI (*se il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica*); INTERESSE PUBBLICO (*se il trattamento è connesso all'esercizio di pubblici poteri);* LEGITTIMO INTERESSE (se il trattamento è necessario per il perseguimento del legittimo interesse dell'INFN e non prevalgano gli interessi degli interessati). La scelta delle opzioni opportune è guidata dall'articolo 6 del GDPR. Si veda l'Appendice 1
Dettagli	Inserire nota di spiegazione che giustifichi le scelte indicate nel campo precedente; ad esempio, le norme di legge nel caso di obbligo legale o di esercizio di pubblici poteri.
Categorie degli interessati	Indicare i soggetti a cui i dati personali si riferiscono. Ad esempio: personale dipendente INFN o collaboratori o fornitori, o altro. Vedi la sezione «Definizioni» di questo documento.

Categorie dei destinatari	Indicare i soggetti ai quali sono comunicati i dati personali. Ad esempio soggetti esterni all'Istituto come istituti esterni per finalità previdenziali, assicurative, bancarie o altro. Vedi la sezione «Definizioni» di questo documento.
Reperimento dei dati	Indicare presso quali soggetti i dati personali sono acquisiti. Ad esempio dall'interessato o da terzi o da altri Servizi o Sedi dell'Istituto. Si rinvia agli n. 13 e n. 14 insieme ai Considerando n. 60, n. 61 e n. 62 riportati in «Appendice 1».
Periodo di conservazione dei dati	Inserire la durata prevista di conservazione dei dati, tenendo presente che il GDPR (articolo 5, paragrafo 1, lettera e) prevede il principio di limitazione della conservazione, stabilendo che i dati personali devono essere conservati solo per il tempo necessario al raggiungimento delle finalità per cui sono stati raccolti. Occorre precisare inoltre se determinati dati personali, invece di essere cancellati esaurita la loro funzione, sono conservati ai fini di archiviazione, precisando in tal caso se in forma anonima o aggregata.
Modalità di conservazione dei dati durante il trattamento e successivamente (se previsto) ai fini di archiviazione.	Inserire una breve descrizione di quanto richiesto.

Individuazione dei dati trattati

Nella sezione seguente vengono individuate le categorie di dati trattati. I campi sono TUTTI richiesti, inserire NO se non vengono trattati dati del tipo indicato.

DATI ANAGRAFICI	Per esempio: nome, cognome, sesso, data di nascita…
DATI DI CONTATTO	Per esempio: indirizzo postale o di posta elettronica, numero di telefono fisso o mobile
DATI RELATIVI ALLA FORNITURA DI UN SERVIZIO DI COMUNICAZIONE ELETTRONICA	Per esempio: dati di traffico, dati relativi alla navigazione internet
DATI DI ACCESSO E DI IDENTIFICAZIONE	Per esempio: username, customer ID,…
DATI DI PAGAMENTO	Per esempio: numero di conto corrente, dettagli della carta di credito,…

DATI RELATIVI A DOCUMENTI DI IDENTIFICAZIONE	Per esempio: carta di identità, passaporto, patente di guida,...
DATI RELATIVI A CONDANNE PENALI E AI REATI O A CONNESSE MISURE DI SICUREZZA E PREVENZIONE	Per dati relativi a condanne penali e reati si intendono, per esempio, sentenze di condanna penale, fedina penale (casellario giudiziale), informazioni su procedimenti penali in corso, sanzioni penali ricevute (es. multe, detenzione). Per dati relativi a misure di sicurezza connesse a reati si intendono, per esempio, restrizioni della libertà personale (es. arresti domiciliari, obbligo di firma), interdizione dai pubblici uffici, sospensione della patente per reati stradali, sorveglianza speciale o misure di prevenzione (es. DASPO, obblighi di soggiorno). Per dati relativi a misure di sicurezza e prevenzione si intendono, per esempio, segnalazioni di polizia per attività criminali sospette, iscrizione a liste di soggetti pericolosi (es. lista nera antiterrorismo, watchlist antimafia), misure di prevenzione per soggetti ritenuti socialmente pericolosi, dati su programmi di protezione testimoni
DATI CHE RIVELINO L'ORIGINE RAZZIALE O ETNICA	Ad esempio: dati anagrafici o documenti ufficiali come luogo di nascita o nazionalità che indichino indirettamente l'origine etnica (es. certificato di nascita, passaporto); Le immagini di una persona possono mostrare tratti somatici come il colore della pelle, il tipo di capelli e le caratteristiche del viso che sono spesso associati a un'origine razziale o etnica; dati biometrici e genetici come test del DNA che indichino l'appartenenza a un gruppo etnico.
DATI CHE RIVELINO OPINIONI POLITICHE	Ad esempio: iscrizione a un partito, o movimento politico, ruoli ricoperti all'interno di un partito (es. segretario, portavoce), partecipazione a manifestazioni, comizi o scioperi con scopi politici, presenza a eventi di campagne elettorali.
DATI CHE RIVELINO CONVINZIONI RELIGIOSE O FILOSOFICHE	Ad esempio: richieste di rinvio concorsi per festività religiose

DATI CHE RIVELINO L'APPARTENENZA SINDACALE	Ad esempio: l'iscrizione a un sindacato, la richiesta di assistenza o tutela legale da parte di un sindacato, la partecipazione ad attività sindacali, ruoli o incarichi sindacali, informazioni sulla trattenuta della quota sindacale in busta paga, richieste di permessi sindacali.
DATI RELATIVI ALLA VITA SESSUALE O ALL'ORIENTAMENTO SESSUALE	Ad esempio: dichiarazioni di appartenenza alla comunità LGBTQ+ e di partecipazione ad associazioni o eventi LGBTQ+, informazioni su relazioni passate o attuali, registri medici con riferimenti all'attività sessuale (es. trattamenti per disfunzioni sessuali, terapie ormonali), reclami per discriminazione basata sull'orientamento sessuale sul posto di lavoro, rettificazioni di sesso.
DATI DI LOCALIZZAZIONE	Ad esempio: dati GPS raccolti da dispositivi elettronici come smartphone o dispositivi portatili, dati di localizzazione derivati da reti e connessioni come la posizione rilevata tramite indirizzo IP, tramite collegamento a reti Wi-Fi e Bluetooth, tramite l'uso di badge di accesso in uffici o edifici, sistemi di videosorveglianza specialmente se dotati di riconoscimento facciale.
DATI DI PROFILAZIONE	Ad esempio: dati relativi attività online, cronologia di navigazione web, ricerche effettuate, interazioni sui social media (like, commenti, condivisioni), cookies e tecnologie di tracciamento, dati sulla frequenza e il tipo di interazioni con siti web o app, analisi dei comportamenti dei dipendenti (es. accessi ai sistemi). Vedi la sezione «Definizioni» di questo documento.
DATI RELATIVI ALLA SALUTE	Vedi definizione nella sezione «Definizioni» di questo documento Ad es: diagnosi e referti medici; anamnesi medica; terapie e trattamenti prescritti; risultati di esami e controlli; cartelle cliniche e fascicoli sanitari.
DATI GENETICI	Vedi definizione nella sezione «Definizioni» di questo documento. Ad es: i risultati di test genetici, come quelli di ascendenza
DATI BIOMETRICI	Vedi definizione nella sezione «Definizioni» di questo documento. Ad es: le impronte digitali, il riconoscimento facciale o la scansione dell'iride

EVENTUALI ALTRI TIPI DI DATI	Nel caso siano presenti altre tipologie di dati non comprese in quelle precedenti specificare quali, altrimenti indicare NO

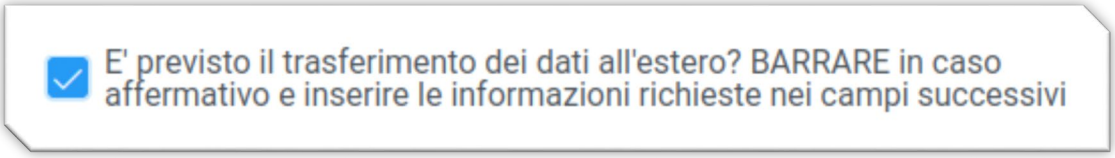
TRASFERIMENTO DATI ALL'ESTERO

Questa sezione è dedicata al trasferimento di dati all'estero.

Le norme sul trasferimento internazionale dei dati sono stabilite dagli articoli 44 e 50 del GDPR.

Se il trasferimento non è previsto passare alla sezione successiva (impatto del trattamento)

Se invece è previsto il trasferimento di dati all'estero spuntare la casella



e riempire i campi successivi.

Trasferimento previsto in UE/SSE	Indicare: • il paese, • i dati trasferiti, • le finalità del trasferimento. Attualmente i paesi appartenenti all'Unione Europea [3] (UE) sono: **Belgio, Bulgaria, Repubblica Ceca, Danimarca, Germania, Estonia, Irlanda, Grecia, Spagna, Francia, Croazia, Italia, Cipro, Lettonia, Lituania, Lussemburgo, Ungheria, Malta, Paesi Bassi, Austria, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia e Svezia**. Attualmente lo Spazio Economico Europeo[4] (SSE) raggruppa i 27 stati membri dell'Unione Europea e tre stati membri dell'Associazione Europea di Libero Scambio (EFTA): Islanda, Liechtenstein e Norvegia.

[3] https://eur-lex.europa.eu/IT/legal-content/glossary/member-states.html
[4] https://eur-lex.europa.eu/IT/legal-content/glossary/european-economic-area-eea.html

Trasferimento previsto in un paese EXTRA UE/SEE in grado di offrire un livello adeguato di protezione	Indicare: • il paese, • i dati trasferiti, • le finalità del trasferimento, • il motivo per cui il paese offre un adeguato livello di protezione. Per i paesi indicati in tale capoverso fare riferimento alle decisioni di adeguatezza, disponibili presso la pagina web del Garante: https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero Alla data del 31/01/2025 la Commissione europea ha adottato decisioni di adeguatezza per i seguenti paesi[5]: **Andorra, Argentina, Canada (organizzazioni commerciali), Isole Fær Øer, Guernsey, Israele, Isola di Man, Giappone, Jersey, Nuova Zelanda, Repubblica di Corea, Svizzera, Regno Unito, Stati Uniti (organizzazioni commerciali che rientrano nell'accordo-quadro UE-USA sulla privacy dei dati) e Uruguay**. Riguardo al trasferimento di dati personali negli Stati Uniti si rinvia alla comunicazione del Direttore Generale INFN del 13/11/2023, disponibile al link: https://dpo.infn.it/wp-content/uploads/2023/11/AOO_SLC-2023-0000139-trasferimento-dati-USA_signed.pdf

Trasferimento previsto in un paese EXTRA UE/SEE non in grado di offrire un livello adeguato di protezione	Indicare:
	• il paese,
	• i dati trasferiti,
	• le finalità del trasferimento.
	• le **garanzie** (articolo 46 del GDPR), scegliendo uno o più valori della seguente lista:
	  ○ Strumento internazionale e giuridicamente vincolante tra autorità pubbliche,
	  ○ Norme vincolanti d'impresa (Binding Corporate Rules - BCRs),
	  ○ Clausole tipo di protezione adottate.
	• oppure le **deroghe** (articolo 49 del GDPR), scegliendo uno o più valori della seguente lista:
	  ○ consenso,
	  ○ contratto tra titolare e interessato,
	  ○ contratto tra titolare e una terza parte.
	
	In tali circostanze dovrà essere avviata una DPIA, coinvolgendo il DPO.

IMPATTO DEL TRATTAMENTO

In questa sezione viene stimato il livello di impatto di un incidente di sicurezza che causi

- la modifica indesiderata,
- l'accesso illegittimo,
- la perdita

dei dati personali relativi al trattamento e valutata la necessità di una DPIA.

Indicare il livello di impatto derivante dalla modifica indesiderata o dall'accesso illegittimo o dalla perdita dei dati oggetto di questo trattamento in caso di incidenti informatici, eventi catastrofici o problemi di varia natura.

Impatto derivante dalla modifica indesiderata/accesso illegittimo/perdita dei dati

BASSO	Piccoli inconvenienti superabili senza particolari problemi (tempo necessario per re-inserire informazioni, irritazione, ecc.)
MEDIO	Inconvenienti significativi, superabili con alcune difficoltà (costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.)
ALTO	Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà (sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato di salute, ecc.)
MOLTO ALTO	Conseguenze significative o irreversibili, non superabili (perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)

*Verifica dei casi che impongono la redazione di una DPIA (**Data Protection Impact Assessment**)*

Nei casi in cui il trattamento comporta "*un rischio elevato per i diritti e le libertà delle persone fisiche*" il GDPR (art. 35) impone di procedere ad un approfondimento delle operazioni di trattamento che si traduce in una apposita procedura denominata (Data Protection Impact Assessment).

Il Garante ha previsto l'obbligo di avviare tale procedura al verificarsi di almeno due delle condizioni descritte nella tabella che segue. Nell'ipotesi in cui si verifichi la sussistenza di una sola condizione resta al Titolare la valutazione di opportunità di procedere con una DPIA. Tale valutazione dovrà essere fatta insieme al DPO che deve essere contattato sollecitamente (dpo@infn.it).

[5]https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_it

Indicare eventuali caratteristiche del trattamento in oggetto, identificate dal GDPR come particolarmente delicate, scegliendo una o più condizioni presenti nella seguente lista.

Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”.	SI/NO
Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che “hanno effetti giuridici” o che “incidono in modo analogo significativamente su dette persone fisiche”.	SI/NO
Monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o “la sorveglianza sistematica su larga scala di una zona accessibile al pubblico”.	SI/NO
Dati sensibili o dati aventi carattere altamente personale.	SI/NO
Trattamento di dati su larga scala: per numero di soggetti interessati al trattamento (in termini assoluti ovvero espressi in percentuale della popolazione di riferimento), il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento, la durata ovvero la persistenza dell'attività di trattamento, la portata geografica dell'attività di trattamento.	SI/NO
Creazione di corrispondenze o combinazione di insiemi di dati, in particolare a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato.	SI/NO
Dati relativi a interessati vulnerabili quali: i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento.	SI/NO
Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative.	SI/NO
Quando il trattamento in sé “impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto”.	SI/NO
Utilizzo di servizi basati su cloud da parte del settore pubblico prevede l'obbligo della DPIA (EDPB[6] del gennaio 2023).	SI/NO
Altro	Questo campo a compilazione libera permette di annotare eventuali altri aspetti del trattamento ritenuti importanti e non presi in considerazione in precedenza

[6] https://edpb.europa.eu/news/news/2023/edpb-determines-privacy-recommendations-use-cloud-services-public-sector-adopts_en

MISURE DI SICUREZZA

Questa sezione è dedicata alle norme di sicurezza.

Quelle generali risiedono in un documento di sede consultabile tramite questo stesso tool

Di seguito vanno invece inserite EVENTUALI ED ULTERIORI misure specifiche introdotte per questo particolare trattamento. Non devono essere inseriti dettagli tecnici ma solo una breve descrizione

TRATTAMENTO INFORMATICO	Indicare il trattamento informatico specifico, scegliendo una delle seguenti voci: • CRITTOGRAFIA DEI DATI • AUTENTICAZIONE AGGIUNTIVA • BACKUP AGGIUNTIVO su sistemi INTERNI • BACKUP AGGIUNTIVO su sistemi esterni • BUSINESS CONTINUITY • DISASTER RECOVERY
Breve descrizione delle misure aggiuntive e delle motivazioni che hanno spinto alla loro adozione	Dare una breve descrizione non tecnica delle misure aggiuntive indicate al punto precedente e le motivazioni che hanno richiesto la loro adozione
TRATTAMENTO CARTACEO	Se è in essere un trattamento cartaceo indicare come vengono conservati i documenti. In caso contrario indicare: NON APPLICABILE

Al termine della compilazione dei campi fare click sul pulsante SALVA.

APPENDICE 1 - DEFINIZIONI

L'articolo 4 del Regolamento UE 2016/679, comunemente indicato come GDPR ("General data protection regulation", in italiano "Regolamento generale sulla protezione dei dati" RGPD) riporta le definizioni dei termini utilizzati nel regolamento stesso. Segue un estratto di tale lista, utile al presente documento.

Dato personale e interessato (art.4, punto 1)	"Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale."
Trattamento (art.4, punto 2)	"Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi 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."
Profilazione (art.4, punto 4)	"Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica."
Pseudonimizzazione (art.4, punto 5)	"Il trattamento 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, a condizione che tali informazioni aggiuntive siano 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."
Archivio (art.4, punto 6)	"Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico."

Titolare del trattamento (art.4, punto 7)	"La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri."
Responsabile del trattamento (art.4, punto 8)	"La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
SUB-responsabile (non è presente una definizione esplicita nell'art. 4)	Nel GDPR il concetto di sub-responsabile del trattamento non è esplicitamente definito come un termine a sé stante, come avviene per esempio per il titolare del trattamento, ma viene regolato nell'articolo 28. In particolare, il paragrafo 2 dell'Articolo 28 stabilisce che: "Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche." Inoltre, il paragrafo 4 specifica che: "Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile."

	Quindi, il sub-responsabile del trattamento è un soggetto terzo che viene incaricato dal responsabile del trattamento per svolgere specifiche attività di trattamento dei dati, ma resta sotto la responsabilità del responsabile principale.
COtitolare (non è presente una definizione esplicita nell'art. 4)	Nel GDPR il concetto di contitolarità del trattamento è definito nell'articolo 26 dove viene specificato che: "1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. 2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. 3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento."
Destinatario (art.4, punto 9)	"La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento".
Terzo (art.4, punto 10)	"La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile."

Consenso dell'interessato (art.4, punto 11)	"Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento."
Violazione dei dati personali (art.4, punto 12)	"La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati."
Dati genetici (art.4, punto 13)	"I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione."
Dati biometrici (art.4, punto 14)	"I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici."
Dati relativi alla salute (art.4, punto 14)	"I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute."
BASE GIURIDICA DEL TRATTAMENTO "CONSENSO" lettera a) del punto 1 art. 6	"l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità". Nei "Considerando" allegati al GDPR si trova inoltre: Considerando n. 42: "Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di prestare un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un

	consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio". Considerando n. 43: "Per assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione".
BASE GIURIDICA DEL TRATTAMENTO "CONTRATTO" lettera b) del punto 1 art. 6	La voce fa riferimento alla: "il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso". ▪ Nel Considerando n. 44 allegato al GDPR si trova inoltre: "Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto".
BASE GIURIDICA DEL TRATTAMENTO "OBBLIGO LEGALE" lettera c) del punto 1, art. 6	La voce: "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento". Nel Considerando n. 45 allegato al GDPR si trova inoltre: "È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro. Il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente

	come base per più trattamenti effettuati conformemente a un obbligo giuridico cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale”.
BASE GIURIDICA DEL TRATTAMENTO “SALVAGUARDIA INTERESSI VITALI” lettera d) del punto 1, art. 6	La voce: “il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica”. Nel Considerando n. 46 allegato al GDPR si trova inoltre: “Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana”.

BASE GIURIDICA DEL TRATTAMENTO “INTERESSE PUBBLICO” lettera e) del punto 1, art. 6	La voce: “il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento”. Nei Considerando n. 45 e n. 46 allegati al GDPR (già riportati sopra) si trovano altre indicazioni riguardo a questa voce.
BASE GIURIDICA DEL TRATTAMENTO “LEGITTIMO INTERESSE” lettera f) del punto 1, art. 6	La voce: “il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.”. Nei Considerando allegati al GDPR si trova inoltre: Considerando n. 47: “I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini

	di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto". Considerando n. 48: "I titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo". Considerando n. 49: "Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica". Considerando n. 50: "Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del

	trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto".

APPENDICE 2

Comunicazione del Direttore Generale INFN del 13/11/2023 riguardo al trasferimento di dati personali negli Stati Uniti, consultabile al link

https://dpo.infn.it/wp-content/uploads/2023/11/AOO_SLC-2023-0000139-trasferimento-dati-USA_signed.pdf

INFN
Istituto Nazionale di Fisica Nucleare
IL DIRETTORE GENERALE

INFN
AOO_SLC-2023-0000139
del 13/11/2023

Ai Direttori delle Strutture INFN

Ai Direttori delle Direzioni e Servizi dell'AC

Al Servizio di Presidenza

All'Ufficio Comunicazione

Ai Presidenti delle Commissioni Scientifiche Nazionali

Ai Presidenti di:
- Commissione Nazionale Calcolo e Reti
- Comitato di Coordinamento della III Missione
- Comitato Nazionale per il Trasferimento Tecnologico
- Comitato Unico Garanzia

Oggetto: trasferimento di dati personali negli Stati Uniti

1. Il trasferimento dei dati all'estero. Come è noto i trasferimenti di dati personali verso paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE, Norvegia, Liechtenstein e Islanda) sono consentiti alle condizioni previste dall'art. 45 del GDPR: una di queste, di carattere generale, prevede che la Commissione europea adotti una decisione di adeguatezza che stabilisca che un paese terzo (ossia un paese non vincolato dal GDPR) garantisce un livello adeguato di protezione dei dati personali. La decisione di adeguatezza consente il trasferimento di dati personali dagli organismi soggetti al GDPR al paese terzo interessato senza ulteriori e particolari adempimenti.

2. Il trasferimento dei dati in USA. Nel luglio 2020 una sentenza della Corte di Giustizia dell'Unione Europea, nota come *Schrems 2*, ha annullato la decisione di adeguatezza adottata nel 2016 riguardo il trasferimento di dati personali verso gli Stati Uniti, rendendo così particolarmente gravosa tale attività: si richiedeva infatti ai titolari di verificare, caso per caso e, ove opportuno in collaborazione con il destinatario dei dati, se la legislazione del paese garantisse un livello di protezione dei dati trasferiti sostanzialmente equivalente a quello vigente nella SEE.
Questo regime è stato recentemente superato a seguito di una nuova decisione di adeguatezza, adottata il 10 luglio 2023 dalla Commissione europea.

3. Le condizioni da rispettare per il trasferimento dei dati negli Usa. Il trasferimento dei dati personali negli Stati Uniti è dunque ora consentito senza ulteriori adempimenti ma solo verso quelle organizzazioni che partecipano al *Data Privacy Framework Program* (DPF), impegnandosi annualmente e pubblicamente ad aderire al quadro giuridico delineato dal GDPR e a rispettarne tutti i principi. L'elenco delle organizzazioni aderenti è disponibile sul sito del DPF.

I trasferimenti alle organizzazioni statunitensi che non aderiscono al DPF non possono essere basati sulla riferita decisione di adeguatezza e richiedono pertanto garanzie adeguate. In particolare, è possibile effettuare il trasferimento incorporando o allegando il testo delle clausole contrattuali standard nell'atto che prevede tale trasferimento, oppure avvalendosi di uno degli altri strumenti elencati nell'articolo 46 del GDPR, quali l'adozione di codici di condotta o di meccanismi di certificazione unitamente all'impegno del titolare o responsabile del trattamento statunitense di applicare le adeguate garanzie.

Istituto Nazionale di Fisica Nucleare
codice fiscale 84001850589
AC - via E. Fermi, 54 - 00044 FRASCATI (Roma) Italia - http://www.ac.infn.it
tel. +39 06 94032477/2496 - fax +39 06 9417007 - email: legale@lnf.infn.it
PEC: amm.ne.centrale@pec.infn.it

Istituto Nazionale di Fisica Nucleare
IL DIRETTORE GENERALE

INFN
AOO_SLC-2023-0000139
del 13/11/2023

I destinatari della presente sono dunque invitati a ricordare ai propri referenti che, prima di procedere al trasferimento di dati personali verso gli Stati Uniti, sono tenuti ad assicurarsi che l'organizzazione ricevente i dati aderisca al DPF, lasciando traccia documentata della ricerca o, nel caso contrario, ad avvalersi delle ulteriori garanzie come sopra individuate, richiamandole esplicitamente nell'atto che prevede tale trasferimento.

Per ogni ulteriore informazione e chiarimento si invita a contattare il Data Protection Officer INFN al seguente indirizzo di p.e.o: dpo@infn.it

Nando Minnella

sottoscritto elettronicamente
Firmato da
Nando Minnella
IT
in data
10-11-2023

Istituto Nazionale di Fisica Nucleare
codice fiscale 84001850589

AC - via E. Fermi, 54 - 00044 FRASCATI (Roma) Italia - http://www.ac.infn.it
tel. +39 06 94032477/2496 - fax +39 06 9417007 - email: legale@lnf.infn.it
PEC: amm.ne.centrale@pec.infn.it