Norme per il trattamento di dati personali nell'INFN

4 Dicembre 2018

PREMESSA

Questo documento contiene le istruzioni per il trattamento dei dati personali nell'Istituto Nazionale di Fisica Nucleare (di seguito anche INFN) in conformità a quanto disposto:

- dal Regolamento UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (di seguito anche Regolamento);
- dal Codice in materia di trattamento dei dati personali di cui al D.Lgs. n. 196/2003 e ss.mm.ii. recante disposizioni per l'adeguamento nazionale al Regolamento UE n. 2016/679 (di seguito anche Codice).

Il personale dipendente ed associato, nonché tutti coloro che collaborano a qualunque titolo nelle attività dell'INFN che comportino il trattamento di dati personali, sono tenuti ad osservarle, conformando la propria condotta a criteri di diligenza e correttezza, al fine di assicurare la massima tutela ai dati trattati.

DEFINIZIONI

Si intende per

- **Dato Personale:** qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamen-

te, 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.

- **Categorie particolari di dati personali:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati relativi a condanne penali e reati:** dati relativi a vicende riguardanti persone fisiche disciplinate dalla legislazione penale, nonché la comminatoria di misure di sicurezza.
- **Trattamento:** 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.

PRINCIPI GENERALI

Il trattamento di dati personali deve essere effettuato nel rispetto dei principi di:

- liceità, correttezza e trasparenza;
- limitazione della finalità del trattamento, assicurando che eventuali trattamenti successivi non siano incompatibili con le finalità per le quali i dati sono stati raccolti;
- minimizzazione dei dati, prestando cura che i dati siano adeguati, pertinenti e limitati a quanto necessario per raggiungere le finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione di quelli che risultino inesatti rispetto alle finalità del trattamento;

- limitazione della conservazione, limitando la conservazione dei dati a un periodo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza, garantendo un'adeguata sicurezza dei dati personali oggetto del trattamento.

I SOGGETTI

I soggetti rilevanti nella disciplina in materia di trattamento dei dati personali sono:

- il Titolare,
- il Responsabile per la protezione dei dati personali,
- i Responsabili del trattamento (eventuali),
- gli Autorizzati al trattamento,
- gli Interessati al trattamento.

Titolare del trattamento dei dati personali: è l'Istituto Nazionale di Fisica Nucleare, cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali. Con deliberazione n. 14844 del 27 luglio 2018 il Consiglio Direttivo dell'INFN ha attribuito:

- al Direttore Generale funzioni di coordinamento per l'attuazione della disciplina in materia di trattamento dei dati personali, assegnandogli, in particolare, il compito di fornire indicazioni di carattere generale, emanare direttive, definire modelli standard delle informative, degli atti di designazione e delle istruzioni, nonché dei contratti di designazione dei Responsabili esterni al trattamento, coordinare la definizione delle misure tecniche ed organizzative volte ad assicurare all'interno dell'INFN il corretto adempimento del Regolamento e la concreta applicazione delle indicazioni provenienti dall'Autorità di controllo;
- ai Direttori delle Strutture dell'INFN, in considerazione dell'attuale organizzazione dei sistemi informativi, il compito di attuare le misure tecniche di sicurezza contenute nell'allegato alla medesima deliberazione, integrandole, se del caso, per assicurare un più efficace livello di sicurezza dei dati personali all'interno della Struttura che dirigono; di assicurare, su base permanente, la riservatezza, la disponibilità e la resilienza dei sistemi esistenti nella Struttura, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la predisposizione e l'esecuzione con rego-

larità di procedure per verificare e valutare l'efficacia delle misure adottate;

- al Direttore Generale, ai Direttori delle Strutture, ai Direttori delle Aree, Direzioni, Divisioni e Servizi Professionali dell'Amministrazione Centrale, di cui all'art. 2 del Disciplinare Organizzativo dell'Amministrazione Centrale, nonché ai Responsabili del Servizio di Presidenza e dell'Ufficio Comunicazione, negli ambiti di rispettiva competenza definiti dagli atti interni dell'Istituto, il compito di assicurare il rispetto di tutti gli obblighi previsti dal Regolamento e dalla normativa nazionale in capo al Titolare del trattamento ed in particolare 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, quali:

  a) designare le persone autorizzate al trattamento dei dati personali nell'ambito della articolazione che dirigono; garantire che le stesse siano state preliminarmente istruite per il trattamento e si siano impegnate alla riservatezza; verificare l'osservanza delle istruzioni che sono state impartite per il trattamento, e, ove ne sussistano le condizioni, l'osservanza di obblighi legali di riservatezza;

  b) assicurare che l'informativa sul trattamento dei dati sia fornita all'interessato e, nei casi previsti, acquisirne il consenso;

  c) dar seguito alle eventuali richieste degli interessati per l'esercizio dei diritti loro garantiti dal Capo IV del Regolamento;

  d) implementare 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;

  e) notificare al Garante della protezione dei dati personali le violazioni dei dati personali (data breach); provvedere alla comunicazione della violazione agli interessati, ai sensi degli articoli 33 e 34 del Regolamento, e darne informativa al Direttore Generale e al DPO;

  f) effettuare, quando sia necessaria e sentito il DPO, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali;

  g) mettere a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi richiesti dal Regolamento; consentire e contribuire alle attività di revisione e di ispezione;

  h) informare immediatamente il Direttore Generale e il DPO in ogni circostanza in cui ritengono che un'istruzione relativa al trattamento dei dati violi il Regolamento o altre disposizioni relative alla protezione dei dati;

i) designare quali Responsabili esterni al trattamento i soggetti che trattano dati personali per conto dell'INFN nell'ambito di convenzioni o contratti che hanno potere a sottoscrivere, nell'ambito delle competenze per valore e materia previste dagli atti interni dell'INFN;

j) individuare un referente locale quale punto di contatto con il DPO e supporto alle attività di gestione degli adempimenti connessi alla protezione dei dati.

Responsabile per la protezione dei dati personali o Data Protection Officier (DPO): è il soggetto designato con deliberazione n. 14734 del 27 aprile 2018 del Consiglio Direttivo dell'INFN, cui è attribuito il compito di:

a) informare e fornire consulenza al Titolare, ai Responsabili del trattamento nonché ai soggetti autorizzati al trattamento circa gli obblighi derivanti dal Regolamento e dalle norme nazionali ed europee relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento e delle altre norme relative alla protezione dei dati, ferme restando le responsabilità del Titolare e del Responsabile del trattamento.

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, pareri in merito alla valutazione di impatto sulla protezione dei dati (*Data Protection Impact Assesment,* DPIA) e sorvegliarne lo svolgimento: a tal proposito il Responsabile per la protezione dei dati indica la necessità di condurre la DPIA sulle singole categorie di trattamento, la metodologia da adottare, le salvaguardie da applicare, comprese le misure tecniche e organizzative per attenuare i rischi delle persone interessate, verificando inoltre se la DPIA sia stata condotta correttamente e se le conclusioni raggiunte siano conformi al Regolamento;

e) cooperare con il Garante per la protezione dei dati personali.

Il Responsabile per la protezione dei dati personali costituisce punto di contatto per gli interessati per tutte le questioni relative al trattamento dei dati personali nell'INFN ed all'esercizio dei diritti garantiti dal Regolamento.

Responsabile del trattamento: è ogni soggetto esterno all'INFN (persone fisiche, giuridiche, altre amministrazioni o autorità pubbliche o altri organismi) che tratta dati per conto dell'INFN.

L'Istituto Nazionale di Fisica Nucleare disciplina i rapporti con il Responsabile del trattamento mediante contratti o altri atti giuridici predisposti secondo i modelli individuati dal Direttore Generale, che vincolano il Responsabile del trattamento al Titolare e individuano l'oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del Titolare e del Responsabile del trattamento.

Autorizzati al trattamento: sono tutti coloro che agiscono sotto l'autorità del Titolare e che hanno accesso ai dati personali; i soggetti autorizzati al trattamento sono istruiti dal Titolare circa le modalità con le quali deve essere effettuato il trattamento.

Interessati al trattamento: sono coloro cui si riferiscono i dati personali trattati.

L'INFORMATIVA

Per adempiere agli obblighi di informazione sul trattamento di cui all'art. 13 del Regolamento, devono essere utilizzati gli schemi di informative disponibili al sito web del DPO dell'INFN.

Nello stesso sito è disponibile anche uno schema di informativa per il trattamento di dati ottenuti da soggetti diversi dai singoli interessati.

È necessario pertanto aver cura che all'avvio di ogni procedimento amministrativo o di qualunque altra attività che coinvolga il trattamento di dati personali sia fornita agli interessati, per iscritto e preferibilmente in formato elettronico, l'informazione preventiva circa:

- il Titolare del trattamento ed i relativi dati di contatto,
- i dati di contatto del Responsabile della Protezione dei dati,
- le finalità e modalità del trattamento,
- i legittimi interessi perseguiti dal Titolare,
- gli eventuali destinatari dei dati,
- l'eventuale trasferimento dei dati in un paese terzo o un'organizzazione internazionale,
- la natura obbligatoria o facoltativa del conferimento dei dati, con indicazione delle conseguenze di un eventuale rifiuto del conferimento stesso,
- il periodo di conservazione dei dati,
- il diritto di chiedere al Titolare l'accesso, la rettifica, o la cancellazione dei dati o la limitazione del trattamento, oltre il diritto di opporsi al loro trattamento,
- l'esistenza eventuale di processi decisionali automatizzati o di profilazione,
- il diritto di presentare un reclamo al Garante per la tutela dei dati personali.

COMUNICAZIONE E DIFFUSIONE DEI DATI

La comunicazione dei dati personali ad un altro soggetto pubblico può essere effettuata quando è prevista da una norma di legge o di regolamento o, in mancanza, se necessaria per lo svolgimento di compiti di interesse pubblico o di funzioni istituzionali, decorsi quarantacinque giorni dalla relativa comunicazione al Garante senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

La diffusione di dati personali trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri a soggetti che intendono trattarli per altre finalità è ammesso solo se previsto da norme di legge o di regolamento

L'art. 100 del Codice consente alle università e gli enti di ricerca, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, di adottare autonome determinazioni con le quali disporre la comunicazione o diffusione, anche a privati e per via telematica, di dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici, tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli di cui agli articoli 9 e 10 del Regolamento.

ISTRUZIONI PER IL TRATTAMENTO DI DATI PERSONALI

Regole generali

I soggetti autorizzati al trattamento devono:

- predisporre la modulistica per la raccolta dei dati personali avendo cura di chiedere agli interessati soltanto i dati necessari e pertinenti alla finalità per le quali sono raccolti;
- accertarsi che la raccolta dei dati personali sia giustificata da una effettiva base giuridica o comunque sia necessaria per eseguire compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è titolare l'INFN;
- nel caso in cui il dato che si intende raccogliere non sia giustificato da una effettiva base giuridica o non sia strettamente necessario per il raggiungimento di compiti di interesse pubblico, far sottoscrivere all'interessato una dichiarazione di consenso al trattamento;

- fornire agli interessati l'informativa sul trattamento in tutte le circostanze in cui procedono alla raccolta di dati personali;
- verificare l'esattezza della scritturazione o digitazione dei dati nelle operazioni di registrazione dei dati personali raccolti;
- utilizzare i dati personali in base al principio del *"need to know"* ed evitare di condividerli o comunicarli a persone che non ne hanno bisogno per lo svolgimento delle proprie mansioni lavorative;
- non trasmettere all'esterno o a soggetti terzi informazioni circa i dati personali conosciuti in ragione della propria attività, salvo che si tratti di comunicazione funzionale allo svolgimento dei propri compiti;
- conservare la riservatezza dei dati personali conosciuti nello svolgimento dell'attività lavorativa anche successivamente al trasferimento ad altra attività o nel periodo successivo alla cessazione del rapporto di lavoro;
- accertarsi dell'identità dell'interessato al momento della raccolta dei dati o prima di fornire informazioni circa i dati personali di altri interessati, anche ove la richiesta sia presentata nell'esercizio del diritto di accesso;
- nei casi in cui è ammessa la consultazione di dati personali e in particolare nei procedimenti di accesso a dati personali, verificare che i documenti oggetto di accesso non riportino dati particolari o dati relativi a condanne penali: in tal caso procedere all'oscuramento di tali informazioni (p. es. mediante *omissis*), salvo che non vi sia una base giuridica che autorizzi la conoscibilità anche di tale tipologia di dati;
- aver cura di non rendere conoscibili, neppure accidentalmente, a soggetti non autorizzati i dati personali contenuti in atti o documenti: a tal fine non lasciare in evidenza documenti quando si ricevono soggetti non autorizzati a conoscere tali dati o non lasciare aperto ed incustodito l'ufficio.

Trattamento con strumenti elettronici

Una buona attenzione alle regole elementari di sicurezza fisica è la base su cui poggiano tutte le altre regole. Per tale motivo è necessario osservare il Disciplinare per l'uso delle risorse informatiche dell'INFN ed in particolare aver cura di:

- accedere ai sistemi di gestione documentale informatizzata e alle banche dati contenenti dati personali soltanto attraverso le credenziali di accesso concesse dall'INFN e nei limiti delle abilitazioni operative consentite dall'Istituto;

- non utilizzare servizi cloud per il trattamento dei dati personali se non espressamente autorizzati dall'INFN;
- se si ha il sospetto che si sia verificato un accesso non autorizzato ai dati personali, segnalare immediatamente l'incidente al Direttore di Struttura o, per l'Amministrazione Centrale, al Direttore di Direzione, Divisione o Servizio di appartenenza;
- fare attenzione, nel caso in cui si utilizzino fotocopiatrici, stampanti o fax condivisi a non lasciare incustodito l'apparecchio con il quale vengono stampati, duplicati o ricevuti documenti contenenti dati personali e rimuovere immediatamente i documenti prodotti; nel caso in cui la stampante o la fotocopiatrice diano segnali di malfunzionamento provvedere a cancellare i lavori in coda, evitando che, a seguito di interventi di manutenzione, il macchinario proceda incustodito alla stampa di documenti contenenti dati personali;
- chiudere le applicazioni che si stavano usando, o attivare il salvaschermo protetto da password, quando si lascia la postazione di lavoro;
- se si trasferiscono dati personali su dispositivi rimovibili (p.e. chiavetta usb), avere cura di cancellarli al termine delle attività di trattamento.

Configurazione del sistema

Tutte le postazioni ed i dispositivi utilizzati per il trattamento di dati personali di cui è Titolare l'INFN devono essere dotati di un antivirus mantenuto costantemente aggiornato. Questo, però, non sempre garantisce una protezione completa (ad esempio per virus molto recenti); è essenziale quindi prestare molta attenzione ad ogni file che si intende aprire o link che si vuole seguire, **specialmente se ricevuti via posta elettronica**.

Le impostazioni del sistema fatte dal Servizio Calcolo non devono essere modificate senza un'autorizzazione preventiva. In particolare è necessario aver cura di:

- non permettere l'esecuzione automatica dei contenuti al momento dell'inserimento di un dispositivo rimovibile;
- attivare l'esecuzione delle macro eventualmente presenti nei file Office solo caso per caso, dopo aver verificato la loro indispensabilità;
- non attivare l'apertura automatica dei link esterni e degli allegati nei messaggi di posta elettronica;
- non attivare l'anteprima automatica dei contenuti dei file;
- non disattivare la scansione automatica anti-malware dei sispositivi rimovibili alla connessione.

Copie di salvataggio

Seguire le indicazioni del Servizio Calcolo in modo che i propri dati vengano salvati con regolarità.

Le password

La corretta individuazione, custodia e gestione delle password consente all'utente di tutelarsi rispetto ad eventuali attività non corrette o addirittura illecite effettuate da altri soggetti tramite il computer a lui assegnato.

La password è personale e l'utente è responsabile della corretta conservazione e gestione della stessa. Non deve essere comunicata ad altri né scritta su supporti facilmente accessibili a terzi. Nella sua scelta devono essere evitati riferimenti personali (nome e/o cognome proprio o di familiari, indirizzo ecc…), e preferite sequenze miste di caratteri e numeri.

I soggetti autorizzati al trattamento dei dati personali devono aver cura, inoltre, di non impiegare la stessa password per i diversi sistemi utilizzati e di non rendere note quelle non più in uso, perché potrebbero permettere l'individuazione delle regole adottate per la loro generazione.

Posta elettronica

I soggetti autorizzati al trattamento dei dati personali non devono mai fornire dati riservati via e-mail (ad es. password). I messaggi in cui vengono richieste informazioni di questo tipo, ad es. tramite un link ad una pagina, anche apparentemente legittima, sono sicuramente dei tentativi di phishing e vanno immediatamente segnalati al Servizio Calcolo.

Prima di aprire un link presente in un messaggio di posta elettronica, verificare con attenzione la sua legittimità, controllando ad esempio l'indirizzo visibile con quello che appare, di solito nella parte inferiore della finestra, quando vi si posiziona sopra il cursore.

Dismissione o reimpiego di apparecchiature elettroniche

I soggetti autorizzati al trattamento dei dati personali devono aver cura, nella dismissione o reimpiego di apparecchiature elettroniche che contengono dati personali, di attuare o far attuare tutte le misure tecniche volte a prevenire accessi non consentiti ai dati personali in esse contenuti mediante un'effettiva cancellazione che garantisca la loro non intelligibilità, secondo quanto disposto dal Garante per la tutela dei dati personali con Provvedimento del 13 ottobre 2008 ed annessi allegati.

Trattamento senza strumenti elettronici

Nel trattamento di dati personali effettuato senza strumenti elettronici (in modo analogico) i soggetti autorizzati al trattamento dei dati personali devono:

- conservare gli atti e i documenti contenenti dati personali soltanto per il tempo necessario alle attività da svolgere e riporli successivamente in archivi ad accesso controllato;
- non lasciare in evidenza sulla scrivania i documenti cartacei quando si ricevono soggetti non autorizzati a conoscere tali dati;
- chiudere a chiave l'ufficio quando ci si assenta;
- non lasciare gli atti e i documenti contenenti dati personali incustoditi su scrivanie o tavoli di lavoro e riporli nei relativi archivi ad accesso controllato a fine giornata;
- se si utilizza carta riciclata, verificare che i fogli non contengano sul retro dati personali;
- ove si renda necessario distruggere documenti contenenti dati personali, utilizzare gli apparecchi distruggi documenti o strapparli in porzioni tali da non essere ricomponibili.

RESPONSABILITÀ E SANZIONI

È riconosciuto il diritto al risarcimento a chiunque subisca un danno materiale o immateriale causato dalla violazione delle norme del Regolamento. Sebbene il risarcimento sia posto a carico del Titolare, questi può esercitare un'azione di rivalsa nei confronti dell'autore del danno, secondo i termini e le modalità previste dalle norme in materia di responsabilità amministrativa.

Nel caso in cui il Titolare dovesse essere assoggettato a sanzioni amministrative è previsto l'accertamento di eventuali responsabilità commesse dal personale autorizzato al trattamento di dati personali.

Per le sanzioni conseguenti a illeciti penali si rinvia all'art. 167 del Codice.

È fatta salva in ogni caso le responsabilità disciplinare eventualmente emergente dalla condotta che ha determinato l'assoggettamento a risarcimento o a sanzione.

CLAUSOLA DI REVISIONE

Il presente documento è aggiornato periodicamente in relazione all'evoluzione della tecnologia e della normativa di settore.