Norme per il trattamento dei dati personali nell'INFN

1 DEFINIZIONI

1.1 IL TRATTAMENTO DEI DATI PERSONALI

Per trattamento dei dati personali si intende qualunque operazione o complesso di operazioni compiute con o senza l'ausilio di processi automatizzati a applicate a dati personali o insieme 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, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati.

1.2 TIPOLOGIE DI DATI

I dati personali si distinguono in *dati personali*, *dati sensibili* e *dati giudiziari*.

Sono **dati personali** (cosiddetti **comuni**) le informazioni relative a persone fisiche, giuridiche, enti od associazioni, identificati o identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Sono **dati particolari** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, nonché i dati genetici e biometrici.

Sono **dati giudiziari** quelli idonei a rivelare provvedimenti di iscrizione nel casellario giudiziale o nell'anagrafe delle sanzioni amministrative dipendenti da reato e i relativi carichi pendenti o la qualità di indagato o di imputato.

1.3 I SOGGETTI

I soggetti rilevanti nella disciplina dettata in materia di trattamento dei dati personali sono il Titolare, i Responsabili e gli Incaricati del trattamento, nonché gli Interessati al trattamento.

Titolare del trattamento dei dati personali è l'Istituto Nazionale di Fisica Nucleare inteso nel suo complesso.

Sono **autorizzati al trattamento** le persone designate ed istruite per compiere operazioni di trattamento dei dati; tra gli iautorizzati, coloro che provvedono alla gestione e/o manutenzione di impianti di elaborazione sono incaricati alla funzione di aAmministratore di sistema.

Responsabili del trattamento dei dati personali sono le persone fisiche o giuridiche o le pubbliche autorità che trattano dati per conto dell'INFN secondo la disciplina individuata in appositi contratti.

Si definiscono **Interessati al trattamento** i soggetti (persone fisiche o giuridiche) cui si riferiscono i dati personali.

2 PRINCIPI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali deve essere effettuato nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dei soggetti cui i dati si riferiscono, con particolare riferimento alla riservatezza, all'identità personale ed alla protezione dei dati personali.

L'Istituto Nazionale di Fisica Nucleare consente il trattamento dei dati personali soltanto per lo svolgimento di attività istituzionali.

Ciascuna operazione di trattamento deve essere effettuata riducendo al minimo l'utilizzazione di dati personali, in modo da escluderne il trattamento quando le finalità perseguite possono essere raggiunte mediante dati anonimi o modalità che consentano il trattamento solo in caso di necessità; tale principio deve essere osservato - in caso di trattamenti effettuati mediante strumenti elettronici - anche nella configurazione di sistemi informativi e programmi informatici.

In ogni caso i dati personali devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono trattati;
- conservati in forma che consenta l'identificazione dell'interessato soltanto per il tempo necessario agli scopi per i quali i dati sono stati raccolti o trattati.

I Responsabili del trattamento individuano per iscritto gli Incaricati e gli amministratori di sistema ed indicano l'ambito di trattamento consentito a ciascuno. Gli stessi Responsabili provvedono alla revoca dell'autorizzazione in tutti i casi in cui vengano meno le condizioni che avevano determinato l'autorizzazione al trattamento (, quali il trasferimento ad altro ufficio, l'assegnazione di altre attività o la cessazione del rapporto di lavoro o collaborazione con l'INFN).

3 INFORMATIVA

Conformemente a quanto previsto dal Regolamento UE 2016/679, l'INFN ha predisposto apposite informative per il trattamento dei dati di personale dipendente e associato, distribuite ai singoli interessati al momento dell'associazione o dell'assunzione. Sono state altresì predisposte informative per le attività di selezione del personale e per l'espletamento delle procedure contrattuali.

In ogni altra circostanza i Responsabili provvedono a fornire, oralmente o per iscritto, agli interessati informazione preventiva circa:

- il Titolare del trattamento ed i 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 una organizzazione internazionale;
- la natura obbligatoria o facoltativa del conferimento dei dati, con indicazione delle conseguenze di un eventuale rifiuto a rispondere;
- il periodo di conservazione dei dati;
- la garanzia del diritto di chiedere al Titolare la rettifica o la cancellazione dei dati o la limitazione del trattamento;
- il diritto di proporre reclamo al Garante per la tutela dei dati personali

4 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; in mancanza di tale norma può essere effettuata quando è comunque necessaria per lo svolgimento di funzioni istituzionali,.

La comunicazione a privati o ad enti pubblici economici e la diffusione sono ammessi esclusivamente quando sono previste da una norma di legge o di regolamento.

In ogni caso i dati idonei a rivelare lo stato di salute non possono essere diffusi.

5 MISURE MINIME DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI

Le misure minime di sicurezza sono costituite dall'insieme delle misure tecniche ed organizzative che l'INFN è tenuto ad adottare al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

I Responsabili del trattamento sono pertanto tenuti ad adottare tutte le misure idonee a ridurre al minimo i rischi sopra indicati e gli iIncaricati del trattamento sono tenuti ad evitare condotte che possano pregiudicare la riservatezza.

5.1 TRATTAMENTO DI DATI EFFETTUATO CON STRUMENTI ELETTRONICITRATTAMENTO DI DATI EFFETTUATO CON STRUMENTI ELETTRONICI

Le risorse informatiche nella disponibilità dei Responsabili ed Incaricati del trattamento devono essere accessibili tramite modalità che consentano, in modo univoco, l'individuazione dell'utente (Responsabile o Incaricato): individuazione che deve avvenire attraverso l'adozione di un meccanismo di autenticazione che si concretizza, quanto meno, nell'uso di un codice identificativo personale (*user-id*) e di una parola chiave (*password*).

LA PASSWLA PASSWORD DI SALVASCHERMO DIRETTA AD IMPEDIRE CHE, IN CASO DI ASSENZA MOMENTANEA DELL'INCARICATO, SOGGETTI NON AUTORIZZATI VISUALIZZINO DOCUMENTI INFORMATICI O COMUNQUE VI ACCEDANO.IN ALCUNI SISTEMI È POSSIBILE ANCHE UTILIZZARE UNA PASSWORD PER IMPEDIRNE L'ACCENSIONE E LE MODIFICHE DELLA CONFIGURAZIONE DI BASE, MA, IN OGNI CASO, IL SUO USO DEVE ESSERE CONCORDATO CON IL SERVIZIO DI CALCOLO E RETI.

5.1.1 MODALITÀ DI SCELTA E GESTIONE DELLE PASSWORD

Una corretta individuazione delle password costituisce un elemento essenziale per la sicurezza e tutela dei dati personali trattati attraverso l'ausilio di strumenti elettronici, dal momento che uno dei metodi più utilizzati per l'accesso illecito ad un sistema o ad una applicazione consiste nell'ottenere ed utilizzare il codice utente e la parola chiave di un utente autorizzato. Al fine di ridurre al minimo tale rischio è necessario pertanto tenere presente che:

- la password è personale e l'utente è responsabile della corretta conservazione e gestione della stessa;
- la password deve avere una lunghezza non inferiore ad 8 (otto) caratteri o al numero massimo di caratteri consentiti dal sistema o applicazione;
- la password deve essere aggiornatamodificata almeno ogni sei mesi ed almeno ogni tre mesi se diretta a concedere l'accesso ad elaboratori, sistemi, applicazioni (data base, cartelle o documenti) che contengano *dati personali sensibili*;

- nella scelta della password devono essere evitati riferimenti personali (nome o cognome proprio o di familiari, indirizzo, ecc…)~~.~~ o parole di senso compiuto in qualsiasi lingua~~ e preferite sequenze miste di caratteri e numeri (ad esempio, utilizzando 3 al posto di E, 0 al posto di O, ! al posto di I, "!PromessiSposi" diventerebbe "!Pr0m3ss!Sp0s!", o, ancora, usando iniziali o spezzoni di parole che compongono frasi, poesie, proverbi, canzoni, espressioni dialettali, "Tanto va la gatta al lardo, che ci lascia lo zampino", potrebbe essere trasformato nella sequenza "TVlGaL,ccLIZ")~~;
- l'utente è tenuto a prendere tutte le misure necessarie ed idonee al fine di evitare che terzi abbiano accesso al suo computer, anche ove si allontanasse durante una sessione di lavoro: in tali circostanze provvederà, ad esempio, ad uscire dall'applicazione in uso e ad attivare ~~sull'elaboratore~~ un salvaschermo protetto da password;
- l'utente deve aver cura di non comunicare ad altri le proprie password~~ (salvo che al soggetto individuato dal Responsabile come custode delle password)~~ e non scriverle su supporti facilmente disponibili a terzi (ad es. collocati in prossimità dell'elaboratore cui si riferiscono);
- l'utente deve aver cura, ~~inoltre~~nel caso siano presenti più sistemi di autenticazione, di non utilizzare la stessa password~~ per le diverse categorie sopra indicate~~ e di non rendere conoscibili ~~password vecchie~~quelle vecchie, anche se non più in uso, poiché da esse ~~è possibile~~potrebbe essere possibile individuare le regole usate ~~dall'utente~~ per la loro generazione.

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.

5.1.2 IL CUSTODE DELLE PASSWORD

Il Responsabile del trattamento dei dati personali provvede all'individuazione per iscritto di uno o più Custodi delle password, in relazione alla complessità organizzativa della Struttura, Direzione o Servizio che dirige. Il ruolo di questa figura ~~e'~~è quello di garantire la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato, laddove sia indispensabile e~~d~~ indifferibile intervenire per necessità operative e di sicurezza del sistema.

Il custode delle chiavi ~~e'~~è in grado di modificare la password dell'incaricato del trattamento poiché ~~é~~è in possesso delle password privilegiate di tutti i sistemi interessati. Laddove si rendesse necessario intervenire nel computer dell'incaricato assente, il Custode modifica la password e permette la realizzazione dell'intervento necessario. Provvede poi ad informare l'incaricato che, una volta rientrato in servizio, ripristina una nuova password personale da lui solo conosciuta.

Modalità ulteriori, anche informatizzate, di gestione delle password potranno essere individuate da ciascun Responsabile del ~~T~~trattamento purché idonee a garantire la disponibilità dei dati solo nel caso in cui, in assenza dell'Incaricato, si renda necessario intervenire immediatamente per garantire la operatività e sicurezza del sistema, con l'obbligo di tempestiva informazione allo stesso incaricato dell'intervento effettuato e ripristino delle nuove password.

5.1.3 MISURE DI PROTEZIONE HARDWARE E SOFTWARE

I Responsabili del trattamento curano che i server disponibili nella propria Struttura, Direzione o Servizio siano ancorati a pareti o pavimenti, localizzati in ambienti caratterizzati da accesso controllato (locali chiusi a chiave) e dotati di sistemi di condizionamento, antincendio ed antiallagamento. Le risorse ritenute critiche devono inoltre essere protette mediante l'installazione di sistemi che garantiscano la continuità dell'energia elettrica.

I Responsabili del trattamento provvedono inoltre, anche mediante i Servizi di Calcolo e Reti, affinché siano installati sistemi anti intrusione informatica, facendo in modo che il loro aggiornamento sia effettuato con cadenza almeno semestrale.

I Responsabili del trattamento curano e verificano, tramite i Servizi di Calcolo e Reti, o le ditte che effettuano l'assistenza informatica, che su tutti gli elaboratori siano installati programmi antivirus in grado di fornire anche una protezione in tempo reale. I programmi devono essere configurati in modo da aggiornarsi automaticamente almeno una volta alla settimana.

Al fine di proteggere gli elaboratori da minacce informatiche gli Incaricati del trattamento sono tenuti in ogni caso ad osservare il ~~d~~*Disciplinare per l'uso delle risorse informatiche dell'INFN*

Formatted: Font: Italic

5.1.4 ~~BACKUP~~COPIE DI SALVATAGGIO

Gli Incaricati del trattamento sono tenuti ad effettuare il salvataggio (*backup*) dei propri file, creando copie di sicurezza al fine di permettere il ripristino, in caso di perdita dei dati, della situazione precedente l'evento dannoso.

Il backup può essere effettuato, secondo le indicazioni fornite dai Servizi di Calcolo e Reti, su specifici server oppure su dischi, nastri o altri supporti rimovibili.

I supporti rimovibili contenenti le copie di ~~backup~~salvataggio devono essere custoditi in armadi chiusi a chiave. Gli stessi supporti non possono essere riutilizzati da altri incaricati, se non dopo che le informazioni in essi contenute siano state rese inintelligibili e comunque non ricostruibili.

Periodicamente, e con frequenza almeno mensile, gli Incaricati sono tenuti ad effettuare prove di ripristino, per verificare la costante adeguatezza delle metodologie adottate e dei supporti di backup utilizzati.

5.2 T~~RATTAMENTO DI DATI EFFETTUATO SENZA STRUMENTI ELETTRONICI~~RATTAMENTO DI DATI EFFETTUATO SENZA STRUMENTI ELETTRONICI

Nel caso in cui i dati personali siano contenuti in atti o documenti cartacei, gli Incaricati dovranno aver cura di custodire tali atti e documenti in modo che non vi abbiano accesso soggetti non autorizzate.

A tal fine gli ~~i~~Incaricati sono tenuti a:

1. ~~ad~~ utilizzare i documenti contenenti dati personali soltanto per il tempo necessario allo svolgimento della propria attività lavorativa, avendo cura di riporre negli archivi i documenti successivamente al compimento delle operazioni di propria competenza;
2. ~~a~~ non lasciare i documenti incustoditi su scrivanie od altro mobilio quando ci si allontana dall'ufficio, provvedendo a chiudere la stanza, in caso di assenza prolungata;
3. ~~a~~ conservare i documenti contenenti dati sensibili o giudiziari in armadi chiusi a chiave o ~~-~~comunque in archivi ad accesso controllato;
4. ~~a~~ conservare, in particolare, i documenti contenenti dati attinenti la salute e la vita sessuale separatamente dagli altri.

6 RESPONSABILITÀ E SANZIONI

Il Decreto Legislativo 30 giugno 2003 - *Codice in materia di protezione dei dati personali* - dispone che chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile se non prova di aver adottato tutte le misure tecniche ed organizzative idonee ad evitare il danno: al fine di fornire tale prova è pertanto assolutamente necessaria la scrupolosa osservanza di tutte le misure di sicurezza dettate in attuazione della disciplina in materia di tutela dei dati personali.

Lo stesso D. Lgs. n. 196/03 prevede inoltre sanzioni penali per il caso di mancata adozione delle misure minime di sicurezza, per il trattamento illecito dei dati personali, nonché sanzioni amministrative per il caso di omessa o inidonea informativa agli interessati.

Si ricorda, da ultimo, che la mancata adozione delle misure indicate, costituendo inosservanza di disposizioni di servizio, può determinare l'assoggettamento a sanzioni disciplinari.