SAPIENZA
UNIVERSITÀ DI ROMA

ALLEGATO 2

ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI

Con questo documento si intende offrire:

- una precisazione in ordine ai termini ed ai concetti più frequentemente richiamati dalla normativa sulla privacy;
- l'esposizione dei principi basilari che ciascun operatore (titolare, responsabile ed incaricato) deve tener presenti per agire in conformità alle prescrizioni richiamate dalla legge in tema di trattamento dei dati personali, compresi quelli sensibili;
- l'indicazione delle misure minime di sicurezza da adottare nel trattamento dei dati personali, che devono essere predisposte tutte e obbligatoriamente, senza essere sottoposte ad alcuna valutazione discrezionale.

TERMINOLOGIA RICHIAMATA FREQUENTEMENTE DALLA LEGGE

Si intende per:

- ***"trattamento"****, qualunque operazione o complesso di operazioni effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati;* in sostanza la legge vuole indicare, con tale termine, la utilizzazione dei dati da parte dell'operatore;
- ***"dato personale"****, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;* sono pertanto dati personali il nome, il cognome, la data di nascita, il codice fiscale, la denominazione sociale, la partita iva; sono considerati dati personali anche quelli relativi al traffico telefonico, alle e-mail ed ai file di log, ossia quei dati che consentono di sapere quando, con chi e per quanto tempo ci si è collegati in rete;
  dai dati personali appena descritti, che sono considerati dati "comuni" si distinguono i:
- ***"dati sensibili"****, ossia 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;*

Università degli Studi di Roma "La Sapienza"
CF 80209930587 PI 02133771002
Area Affari Istituzionali – Settore Affari Generali
Piazzale Aldo Moro n. 5 – 00185 ROMA
T (+39) 06 4991 0618 – 0343 F (+39) 06 4991 0216
affgen-arai@uniroma1.it

- ***"dati giudiziari"**, ossia i dati personali idonei a rivelare provvedimenti di cui all'art. 3 comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14/11/02, n.313, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del C.P.P.;* essi riguardano alcune informazioni concernenti il rapporto tra il cittadino e la giustizia penale, come, per esempio, le condanne penali passate in giudicato, la sospensione condizionale e la non menzione della pena, le misure di sicurezza personali e patrimoniali.

Vi sono poi le figure del:

"titolare" del trattamento è *la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali ed agli strumenti utilizzati*; nel caso dell'Università, è tale la struttura nel suo complesso, riconducibile alla figura che ne detiene la rappresentatività giuridica, ossia il Rettore *pro tempore*;

- ***"responsabile"*** del trattamento ossia *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente*, *associazione od organismo preposti dal titolare al trattamento di dati personali*; considerato cioè che all'interno di una amministrazione o azienda le competenze possono essere variegate e distanti tra loro, la legge consente al titolare di nominare "responsabili del trattamento" relativi a determinati rami di attività, con il compito di sovrintendere alle operazioni di trattamento e di assicurare che vengano rispettati determinati requisiti di sicurezza; per l'Università i responsabili del trattamento sono individuati nelle figure dei preposti alle strutture didattiche (es. Presidi di Facoltà) e dei preposti alle strutture amministrative (es. Direttore Generale, Direttori di Area e titolari di Uffici di livello equivalente);
- ***"amministratori di sistema"*** *sono le persone fisiche incaricate del trattamento dei dati che operano in regime speciale, in ragione dei privilegi informatici detenuti*, per cui sono concretamente "responsabili" di specifiche fasi lavorative che possono comportare un elevato livello di criticità rispetto alla protezione dei dati;
- ***"incaricati"*** *sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile* e quindi tutti gli operatori che, nell'ambito di un rapporto di lavoro a tempo indeterminato o meno o nella qualità di collaboratori esterni, quotidianamente o saltuariamente effettuano il trattamento dei dati; in proposito si deve considerare che i dati possono essere trattati soltanto da coloro che hanno ricevuto apposito incarico di trattamento e che l'incaricato deve poter accedere soltanto ai dati che gli servono per svolgere i propri compiti e non a tutti i dati in modo indiscriminato (l'art.3 del DLgs n.196/2003 esprime il principio di necessità precisando che i sistemi informativi riducono al minimo l'utilizzazione di dati personali). In particolare, ove si ritenga opportuno individuare profili di autorizzazione diversi per l'accesso ai dati,

dovranno essere conferiti appositi incarichi a singoli o a classi omogenee di incaricati; in questo caso il profilo di autorizzazione al trattamento dei dati informatici deve rispecchiare l'ambito dell'incarico conferito.

- ***"interessato"*** *è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;* e cioè il soggetto che ha interesse a che i dati vengano trattati in modo lecito e secondo correttezza;
- ***"comunicazione"*** *è il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati; in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*
- ***"diffusione"*** *è il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*
- ***"blocco"*** *è la conservazione dei dati personali con sospensione temporanea di ogni altra operazione del trattamento;*
- ***"banca di dati"*** *è qualsiasi complesso organizzato di dati personali, ripartito in una o più unità, dislocato in uno o più siti;* quindi costituiscono "banche" i dati contenuti in un p.c., in più p.c. connessi ad una unità centrale, in un supporto rimovibile, in un archivio cartaceo e così via;
- ***"Garante"*** *è l'autorità di cui all'art. 153 del D.Lgs. n.196/2003, istituita dalla Legge n. 675 del 31/12/1996;*
- ***"misure minime di sicurezza"*** sono il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali previste dal DLgs n. 196/2003 negli articoli 33, 34 e 35 e che trovano nel disciplinare tecnico - Allegato B al Decreto (anche questo è consultabile sul sito www.garanteprivacy.it) l'attuale traduzione tecnica, la quale potrà essere modificata nel corso degli anni; esse vengono ritenute dalla legge essenziali per assicurare il livello minimo di protezione dei dati personali e debbono essere quindi necessariamente ed integralmente adottate. Si distinguono in misure concernenti i trattamenti con strumenti elettronici (adozione delle credenziali di autenticazione, costituite da un codice identificativo e da una password segreta; scadenza degli account; backup dei dati; antivirus; aggiornamenti dei software; protezione perimetrale della rete; formazione degli incaricati; profili di autorizzazione, ossia definizione degli ambiti di accesso ai dati consentiti a ciascun incaricato ovvero a classi di incaricati) e misure concernenti i trattamenti senza l'ausilio di strumenti elettronici (idoneità dei locali e degli armadi; identificazione e registrazione di chi accede ai locali ove sono custoditi dati sensibili dopo l'orario di lavoro);
- **"*custode della parola chiave*"** è la figura individuata dal punto 10 del citato disciplinare tecnico per assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato. Questa figura, che deve essere nominata dal responsabile preventivamente e per iscritto, deve conservare in busta sigillata le credenziali di autenticazione di ciascun incaricato in modo tale da garantirne la segretezza e deve informare senza ritardo l'incaricato qualora si sia reso necessario effettuare un intervento.

PRINCIPI BASILARI PER IL RISPETTO DELLE NORME

Occorre ora puntualizzare alcune regole generali imposte dalla legge in relazione al trattamento dei dati; esse devono costituire il principale punto di riferimento per il titolare, per il responsabile e per l'incaricato del trattamento:

a) la raccolta dei dati personali deve essere preceduta dalla informativa agli interessati, cioè dalla comunicazione di tutte le notizie concernenti la finalità, la obbligatorietà o facoltatività del conferimento, le conseguenze del rifiuto di rispondere, i soggetti ai quali i dati possono essere comunicati, gli estremi identificativi del titolare e del responsabile, i diritti che gli interessati stessi possono esercitare ai sensi dell'art. 7 del Codice (diritto di ottenere informazioni su tutti i punti sopraindicati ed inoltre di ottenere l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, il blocco e la trasformazione in forma anonima dei dati, ossia l'immissione del proprio dato in un ambito in cui venga trattato in modo aggregato con altri).
   Questo insieme di regole ha lo scopo di costruire con l'utente dei servizi un rapporto il più possibile improntato al criterio della trasparenza, in quanto diretto a consentire la conoscenza dei principi posti a base del trattamento.
   E' bene tuttavia specificare che l'Università, come ogni altro Ente Pubblico, ha l'obbligo di informare preventivamente, ma non quello di chiedere il consenso al trattamento.
   Inoltre i dati devono essere:
b) trattati in modo lecito e rispondente ai criteri di riservatezza e correttezza; in altri termini è necessario che durante tutte le fasi di utilizzazione venga effettuata una vigilanza continua diretta a garantire la riservatezza dei dati, ad evitarne la destinazione a fini illeciti o comunque la gestione con modalità non professionalmente corrette;
c) raccolti e registrati per scopi esclusivamente attinenti alle finalità dell'Università, utilizzati in altre operazioni del trattamento in termini compatibili con tali finalità; deve essere quindi impedito ogni tipo di trattamento non conforme alle finalità della raccolta, ma è ipotizzabile un trattamento "confinante" con tale finalità: ad esempio è possibile, previo consenso dell'interessato, comunicare il dato personale di chi abbia conseguito la laurea ad una ditta che abbia manifestato l'intento di fare assunzioni;
d) esatti e, se necessario, aggiornati;
e) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
f) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
g) custoditi e controllati in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, o di accesso non consentito.

La custodia ed il controllo dei dati sono intesi dal Codice come "misure di sicurezza" connesse al trattamento: è indispensabile che l'operatore, nell'eseguire il proprio lavoro, non tenga conto unicamente del fine da perseguire, ma anche della assoluta necessità di premunirsi contro i rischi di perdita o di manipolazione o lettura indebita dei dati. Queste misure non sono predeterminate e stabili; la loro determinazione ed attuazione è demandata ai responsabili delle strutture in funzione delle esigenze e caratteristiche delle strutture stesse (per es. in un determinato ufficio potrebbe essere essenziale disporre il salvataggio dei dati su supporto rimovibile al termine di ogni giornata di lavoro) ed in funzione delle conoscenze acquisite in base al progresso tecnico.

MISURE MINIME DI SICUREZZA

Occorre sottolineare, a questo punto, che gli obblighi di adozione di misure di sicurezza sono duplici: da una parte c'è l'obbligo di predisporre tutte le misure che si ritengono utili secondo quanto si è appena detto; dall'altra c'è l'obbligo di adottare le **"misure minime"** cui si è accennato precedentemente e che sono previste, oltre che dal Codice, dal disciplinare tecnico.
Queste ultime, a differenza delle misure d'ordine generale, non sono più individuabili discrezionalmente ma devono essere adottate tutte e necessariamente; l'inosservanza di questo obbligo posto a carico del titolare, del responsabile e di ogni singolo incaricato — ciascuno per la parte di sua competenza — rende il trattamento illecito anche se non si determina un danno per gli interessati; vìola inoltre i diritti di questi ultimi, compreso il diritto fondamentale alla protezione dei dati personali, ed espone a responsabilità civile per danno anche non patrimoniale.
Le misure minime si distinguono in:

1) Misure minime concernenti i trattamenti CON l'ausilio di strumenti elettronici

La predisposizione di queste misure spetta agli uffici informatici, che agiscono insieme ai responsabili del trattamento. La loro attuazione pratica è poi demandata, almeno in qualche caso (corretta gestione delle credenziali di autenticazione), agli operatori.
Esse sono suddivisibili in **tre aree**:

a) Protezione di dati e sistemi
I dati archiviati su supporto elettronico rimovibile devono essere riposti e custoditi con gli stessi criteri che vengono usati per i dati cartacei.
I dati e i sistemi elettronici devono essere protetti da accessi non consentiti diretti alla compromissione della loro sicurezza.
Devono essere usati ed aggiornati, con cadenza almeno semestrale, strumenti elettronici che contrastino i virus informatici.

Gli aggiornamenti dei programmi devono essere effettuati con cadenza annuale e, se sono relativi a dati sensibili o giudiziari, con cadenza semestrale.
Devono essere usati soltanto i software forniti dalle strutture di appartenenza, è quindi vietato scaricare software dalla rete.
Se un PC o un supporto rimovibile contenente dati sensibili o giudiziari viene destinato ad una nuova persona, bisogna garantire che le informazioni precedentemente in esso contenute non siano in alcun modo intelligibili e non ricostruibili tecnicamente in alcun modo.

b) Autenticazione informatica
Ogni incaricato addetto al trattamento dei dati con strumenti elettronici deve essere dotato di credenziali di autenticazione, ossia di un codice di identificazione personale non condivisibile con altri utenti e di una password segreta; quest'ultima deve essere composta da almeno otto caratteri o comunque dal numero massimo di caratteri consentito, deve essere cambiata dall'incaricato immediatamente dopo la prima utilizzazione e, successivamente, almeno ogni sei mesi se vengono trattati dati comuni **ed almeno ogni tre mesi se vengono trattati dati sensibili o giudiziari,** non deve mai contenere riferimenti agevolmente riconducibili all'incaricato.
Quest'ultimo deve, altresì, consegnare al "custode" nominato dal responsabile del trattamento una busta sigillata recante all'esterno il proprio nome e cognome ed all'interno le credenziali di autenticazione; in caso di necessità dovuta ad assenza od impedimento dell'incaricato, il custode, autorizzato dal responsabile, apre la busta, accede ai dati, informa l'incaricato; quest'ultimo provvede a cambiare la parola chiave immediatamente dopo la ripresa del servizio ed a consegnarla nuovamente in busta sigillata al custode.
L'incaricato, inoltre, nell'operare il trattamento dei dati sotto la diretta autorità del responsabile, deve:

- provvedere, almeno settimanalmente, al salvataggio su supporto rimovibile dei dati presenti soltanto su PC. Tale supporto deve essere custodito adeguatamente in luogo chiuso a chiave;
- custodire la propria password in modo tale che non possa essere conosciuta da altri;
- astenersi dal comunicare i dati anche agli altri incaricati che non siano direttamente coinvolti nello stesso processo di trattamento;
- non lasciare mai incustodito lo strumento elettronico durante una sessione di lavoro in modo tale da impedire che i dati possano essere conosciuti da terzi;
- segnalare per iscritto al responsabile ogni anomalia riscontrata nel trattamento dei dati;
- non aprire messaggi di posta elettronica dei quali non si conosca l'origine;
- collaborare con il responsabile e con gli uffici dell'Amministrazione per consentire la realizzazione di tutte le prescrizioni contenute nel D. Lgs.

n.196/2003 e nel disciplinare tecnico in materia di misure minime di sicurezza nel trattamento dei dati.

c) Sistema di autorizzazione
Se il trattamento dei dati prevede la necessità di utilizzare incaricati con compiti distinti (come nel caso in cui alcuni possono visualizzare i dati e altri possono anche modificarli) deve essere adottato e gestito un sistema di accesso ai dati e ai sistemi basato sui "profili di autorizzazione".
Tali profili devono definire in dettaglio le azioni consentite a ogni classe di incaricati e devono indicare le impostazioni da assegnare agli strumenti elettronici che realizzano i meccanismi di autorizzazione.
La verifica che siano ancora valide le definizioni dei profili di autorizzazione deve essere effettuata periodicamente e, comunque, almeno una volta all'anno.

2) Misure minime concernenti i trattamenti SENZA l'ausilio di strumenti elettronici

Gli incaricati, nell'operare il trattamento dei dati su supporto cartaceo, o comunque diverso da quello elettronico, sotto la diretta autorità del responsabile, devono:

- controllare costantemente la documentazione e non lasciarla mai incustodita durante una sessione di lavoro in modo tale da evitare che i dati ivi contenuti possano essere conosciuti da terzi;
- riporre sempre la documentazione negli appositi luoghi di custodia chiusi a chiave al termine di ogni sessione;
- astenersi dal comunicare i dati anche agli altri incaricati che non siano direttamente coinvolti nello stesso processo di trattamento.

Se i documenti contengono dati sensibili o giudiziari, devono essere riposti e chiusi a chiave in archivi ad accesso controllato; se, per qualsiasi motivo, una persona, dopo l'orario di lavoro, è ammessa in un locale ove sono riposti archivi contenenti dati sensibili o giudiziari, si deve procedere alla sua identificazione e registrazione. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

Per quanto non espressamente previsto nelle presenti istruzioni, si rinvia alle prescrizioni del D. Lgs. n. 196 del 30 giugno 2003 "*Codice in materia di protezione dei dati personali*" e successive modifiche.