La protezione dei dati personali
Attuazione del D. Lgs. 196/2003

MANUALE AD USO DEI RESPONSABILI E DEGLI INCARICATI

Versione: 5.1
Numero totale pagine: 29

ELENCO DEI CONTENUTI

MANUALE AD USO DEI RESPONSABILI E DEGLI INCARICATI

1. INDICAZIONI GENERALI PER IL TRATTAMENTO DI DATI PERSONALI

1.1. I principi e gli obblighi fondamentali

Il primo gennaio del 2004 è entrato in vigore il decreto legislativo 30 giugno 2003, n. 196, recante il "**Codice in materia di protezione dei dati personali**" - d'ora in poi denominato "Codice" - nel quale sono raccolte, in forma di testo unico, tutte le disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ed alle attività connesse. Il Codice sancisce il diritto alla protezione dei dati personali, prerogativa fondamentale della persona, e garantisce che il trattamento di queste informazioni "si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

Il sistema di garanzie approntato dal Codice si ispira ai principi di semplificazione, efficacia ed armonizzazione delle modalità di esercizio dei diritti e delle libertà fondamentali dell'interessato e degli adempimenti degli obblighi da parte dei titolari dei trattamenti *(ar. 2, comma 2)*.

Il Codice introduce pertanto una simmetria tra le disposizioni che disciplinano:

a) le modalità d'esercizio dei diritti degli interessato
b) l'adempimento degli obblighi da parte del titolare del trattamento.

La normativa, dinamica e coerente con gli indirizzi giurisprudenziali più attuali, è improntata ai principi di:

- **Semplificazione**: nella ricerca di percorsi più snelli per le modalità di esercizio dei diritti da parte degli interessati e degli adempimenti da parte del titolare.
- **Armonizzazione**: nello sforzo di creare un sistema privacy pubblico-privato differenziato, ma coerente e di collegarsi in modo coordinato all'intero impianto legislativo vigente, non solo in materia di tutela della privacy.
- **Efficacia**: nel rendere il Codice concretamente operativo, mediante la previsione, accanto alle norme primarie (norme di legge), di norme secondarie di attuazione e di dettaglio (norme di regolamento).

Il diritto alla protezione dei dati personali potrà essere garantito solo se le amministrazioni titolari dei trattamenti ispireranno la loro attività ai principi sanciti dal Codice e conseguentemente, oltre ad ottemperare agli obblighi ivi espressamente previsti, adotteranno una serie di comportamenti concreti, azioni e provvedimenti organizzativi coerenti con i principi che regolano la materia.

1.2. Il significato di alcuni termini introdotti dalla normativa vigente

Il codice definisce dati **personali** "*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*".

Nei sistemi informativi di una organizzazione le informazioni contenenti dati personali sono presenti essenzialmente nelle seguenti forme:

- dati strutturati (ad esempio, database)
- dati destrutturati (ad esempio, documenti o posta elettronica).

E' fondamentale comprendere che la norma protegge i dati personali indipendentemente dalla forma nella quale essi sono organizzati e del supporto utilizzato (sia questo informatico o meno).

I dati **sensibili** sono quelli 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.* Tra i dati sensibili rientrano quelli biomedici e genetici. Pertanto, nell'ambito dell'Ateneo, i dati sensibili concretamente utilizzati sono relativi a:

- appartenenza del dipendente ad associazioni sindacali;
- inabilità del dipendente;
- inabilità del familiare dal dipendente;
- malattia del dipendente;
- provvedimenti giudiziari a carico del dipendente;
- handicap dello studente.

I dati **giudiziari** sono 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 imputato o di indagato.*

Per **trattamento** deve intendersi qualunque operazione o complesso di operazioni, effettuati 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.

Il **titolare** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il **responsabile** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. Ai sensi del Regolamento di Ateneo, i responsabili dei trattamenti dei dati personali, anche sensibili e giudiziari, effettuati dall'Università sono nominati dal Titolare con provvedimento scritto tra il personale responsabile di uffici, strutture e servizi dell'Ateneo.

Gli **incaricati** sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. Ai sensi del Regolamento di Ateneo, gli incaricati dei trattamenti dei dati personali, anche sensibili e giudiziari, effettuati dall'Università sono nominati dai responsabili tra il personale afferente all'ufficio o struttura.

L'**interessato** è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

1.3. Indicazioni generali per il trattamento

Il trattamento dei dati personali da parte delle pubbliche amministrazioni è consentito solo qualora sia necessario per lo svolgimento delle funzioni istituzionali, rispettando gli eventuali altri presupposti e limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti.

I dati sensibili possono, invece, essere trattati soltanto se il trattamento risulta autorizzato da un'espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Nell'effettuare qualsivoglia trattamento, al fine di mantenersi entro gli ambiti della legittimità fissati dal Codice, i responsabili dovranno verificare che il trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali. In particolare, ciascun trattamento dovrà essere effettuato riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

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 raccolti o successivamente trattati;
- 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.

1.4. Consenso e informativa

Si evidenzia che il Codice prevede che i soggetti pubblici e, dunque l'Università, salvo quanto espressamente previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, non devono richiedere il consenso dell'interessato.

Il Codice prescrive inoltre l'obbligo di rendere l'informativa per tutti i trattamenti effettuati. Pertanto, il responsabile dovrà adottare ogni misura organizzativa idonea, ivi compreso l'inserimento dell'informativa

nella modulistica utilizzata nell'ambito della propria struttura, affinché l'interessato o la persona presso la quale sono raccolti i dati personali siano previamente informati per iscritto circa:

- le finalità e le modalità del trattamento cui i dati sono destinati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in quanto responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato;
- gli estremi identificativi del titolare e del responsabile.

Al fine di poter provare in ogni caso di **aver adempiuto all'obbligo di rendere l'informativa**, sebbene il Codice preveda la possibilità di renderla anche solo oralmente, **si dispone che la stessa venga resa sempre per iscritto**.

1.5. Diritti dell'interessato

Sono indicati all'art. 7 del Codice nel quale è previsto che l'interessato ha diritto ad ottenere conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati, e la loro comunicazione in forma intelligibile; ha il diritto di conoscerne la fonte, di sapere per quali finalità e con quali modalità sono trattati, se e a chi detti dati vengono comunicati; ha, inoltre, il diritto di ottenerne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco, con attestazione che dette operazioni sono state portate a conoscenza anche di coloro ai quali i dati sono stati comunicati o diffusi. L'interessato può inoltre sempre opporsi al trattamento dei dati che lo riguardano, in particolare ove esso sia effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Detti diritti sono esercitati con richiesta rivolta, senza formalità, al titolare o al responsabile, anche per il tramite di un incaricato. Alla richiesta deve essere fornito idoneo riscontro senza ritardo.

La richiesta può essere trasmessa anche mediante fax o posta elettronica o semplicemente formulata in via orale. Quando essa riguarda la mera richiesta di informazioni relative al trattamento eventualmente in atto, può essere formulata anche oralmente; in tal caso è annotata sinteticamente a cura del responsabile o dell'incaricato.

Al fine di esaudire la richiesta dell'interessato il responsabile, o un incaricato all'uopo individuato, dovrà:

- comunicare oralmente le informazioni richieste;

oppure

- consentire la visione delle informazioni mediante strumenti elettronici;

oppure

- se richiesto, provvedere alla trasposizione dei dati su supporto cartaceo o informatico ovvero all'invio per via telematica.

1.6. Comunicazione e diffusione di dati personali

La **comunicazione** e la **diffusione** di dati personali costituiscono trattamenti particolarmente delicati. Si ritiene utile, pertanto, richiamare l'attenzione dei responsabili sulle disposizioni da osservare, coerentemente con quanto disposto dal "Regolamento di Ateneo di attuazione del codice di protezione dei dati personali" (D. R. n. 5073 del 31.05.2007), nel prosieguo detto Regolamento di Ateneo.

La comunicazione dei dati nell'ambito dell'Ateneo è ispirata al principio della libera circolazione delle informazioni. La comunicazione ad altro soggetto pubblico è invece ammessa o quando è prevista da una norma di legge o di regolamento oppure quando è comunque necessaria per lo svolgimento di funzioni istituzionali dell'ente richiedente. In tale ultimo caso, il responsabile – per il tramite del Titolare - è tenuto a darne comunicazione al Garante, a mezzo telefax o con altro mezzo idoneo ad attestarne la ricezione; la comunicazione può essere avviata decorso il termine di quarantacinque giorni dalla comunicazione del trattamento al Garante.

La comunicazione a privati o a enti pubblici economici di dati personali diversi da quelli sensibili e giudiziari è regolata dall'art. 13 del Regolamento di Ateneo e può avvenire solo dietro richiesta scritta e motivata. Tale richiesta, indirizzata al Titolare, deve contenere le seguenti indicazioni:

a. il nome, la denominazione, la ragione sociale;
b. i dati di cui si richiede la visione o la trasmissione;
c. le finalità e le modalità di utilizzo dei dati richiesti;
d. l'eventuale ambito di comunicazione dei dati richiesti;
e. l'eventuale connessione con altri trattamenti e/o banche dati.

La diffusione di dati personali sensibili e giudiziari non è mai ammessa. La diffusione di dati personali diversi da quelli sensibili e giudiziari è invece ammessa unicamente quando sono previste da norma di legge o di regolamento, richiamando la quale il trattamento potrà essere effettuato. In ogni caso, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

1.7. Le responsabilità e le sanzioni

All'interno del Codice vige il principio della responsabilità oggettiva per il trattamento dei dati personali. In base a questo principio, chiunque (responsabile o incaricato, in relazione ai rispettivi ambiti di responsabilità) cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'*art. 2050 c.c. (responsabilità derivante dall'esercizio di attività pericolose)* se non prova di aver adottato tutte le misure tecniche ed organizzative idonee ad evitare il danno.

Al fine di poter fornire tale prova, risulta indispensabile per i responsabili e per gli incaricati di trattamento osservare scrupolosamente le istruzioni individuate dal Titolare in attuazione della normativa in materia di protezione dei dati personali.

Si evidenzia, altresì, che, in ogni caso, la violazione di disposizioni del Titolare costituisce violazione dei doveri d'ufficio ed implica, conseguentemente l'applicabilità di sanzioni disciplinari.

Fra le tante sanzioni previste dal Codice si ritiene inoltre opportuno, segnalare che:

- la omessa o inidonea informativa all'interessato, la cessione di dati al di fuori dei casi consentiti, la violazione delle disposizioni in tema di comunicazione di dati personali idonei a rivelare lo stato di salute o la vita sessuale nonché l'omessa informazione o esibizione di documenti al Garante comportano l'applicabilità di una sanzione amministrativa;

- il trattamento illecito di dati, la falsa notifica o false informazioni al Garante, l'omessa adozione delle misure minime di sicurezza e l'inosservanza dei provvedimenti del Garante costituiscono per il trasgressore illecito penale;
- come pena accessoria è sempre prevista la pubblicazione della sentenza di condanna.

1.8. Sicurezza dei dati e dei sistemi

Ai sensi dell'art. 33 e dell'art. 34 del Codice, il trattamento dei dati personali è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B del Codice, le seguenti misure minime di sicurezza, distinte a seconda che il trattamento sia effettuato con o senza l'ausilio di strumenti elettronici:

1.8.1. Trattamenti effettuati con l'ausilio di strumenti elettronici

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico (**almeno annuale**) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

1.8.2. Trattamenti effettuati senza l'ausilio di strumenti elettronici

a) aggiornamento periodico (**almeno annuale**) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

In ogni caso, qualunque sia la tipologia di trattamento effettuato, l'omissione da parte di chiunque (responsabile o incaricato) dell'applicazione delle misure minime di sicurezza è sanzionabile penalmente, in base a quanto sancito dall'art. 169 del Codice. Inoltre, l'adozione di misure di sicurezza inadeguate (cioè non coerenti con quanto disciplinato dal Codice o dalla legge) rende il trattamento illecito, per cui il titolare non può più utilizzare i dati raccolti e l'interessato può ottenerne la cancellazione.

2. GLI ADEMPIMENTI PER IL RESPONSABILE

2.1. La nomina degli incaricati

Qualora siano gestiti dati **personali**, il responsabile del trattamento dei dati dovrà autorizzare per iscritto gli incaricati ed assegnare loro il relativo ambito di trattamento coerente con quanto riportato nell'ultima versione pubblicata della tabella Ambiti_Trattamento della propria struttura[1], procedendo alla revoca della detta autorizzazione in tutti i casi di perdita della qualità che consente all'incaricato l'accesso ai dati personali (per es.: per trasferimento del dipendente ad altro ufficio, per assegnazione ad altre attività, per estinzione del rapporto di lavoro con l'Ateneo).

Per il conferimento e la revoca dell'incarico, il responsabile dovrà utilizzare:

a. il modello SICURDAT/A per autorizzare i trattamenti cartacei o elettronici su PC non in rete,
b. il modello SICURDAT/B per autorizzare i trattamenti automatizzati centralizzati.

In ogni caso, sul modulo dovrà essere apposta anche la firma dell'incaricato del trattamento per attestare l'avvenuta comunicazione dell'incarico a lui affidato e dell'ambito di trattamento che gli è consentito. I due modelli SICURDAT sono reperibili all'indirizzo: http://www.unina.it/attiNorme/sicurezza/index.jsp.

Tali moduli, anche in assenza di variazioni, quindi con la conferma degli incarichi e dell'ambito di trattamento consentito a ciascun incaricato, dovranno comunque essere inviati ogni anno alla Direzione Amministrativa.

Nel caso di comunicazione all'esterno dell'Ateneo di dati personali (mediante trasmissione di flusso cartaceo o elettronico, oppure mediante l'utilizzo di specifiche applicazioni informatiche non gestite dall'Ateneo) si evidenzia l'importanza di segnalare, nel modello SICURDAT/A, la denominazione dei soggetti o degli enti esterni a cui i dati sono comunicati e dell'applicazione utilizzata. Il responsabile deve segnalare queste informazioni anche nel caso di accesso a banche dati esterne gestite da applicazioni informatiche dell'ente o soggetto esterno.

All'atto del conferimento dell'incarico, il responsabile deve consegnare all'incaricato il presente manuale (reperibile anche all'indirizzo: http://www.unina.it/attiNorme/sicurezza/index.jsp), in quanto contiene - tra l'altro - le istruzioni, le regole e le prassi a cui devono attenersi gli incaricati per la tutela dei dati personali trattati dall'Università degli Studi di Napoli Federico II.

2.2. L'aggiornamento dell'ambito di trattamento

Con frequenza annuale, ciascun responsabile deve provvedere a comunicare alla Direzione Amministrativa eventuali difformità riscontrate fra quanto risulta dalla tabella Ambiti_Trattamenti in cui

[1] Per le ripartizioni e gli uffici dell'Amministrazione Centrale, la tabella è denominata Ambiti_Trattamenti; per gli uffici dei Poli è denominata Ambiti_Trattamenti_Poli; per le strutture didattiche, di ricerca e di servizio dell'Ateneo, è denominata Ambiti_Trattamento_Strutture_Ateneo.

risulta censita la propria struttura (o ufficio) e la situazione di fatto esistente nella struttura stessa (o ufficio), al fine di evitare la violazione della normativa vigente per quanto attiene alla erronea individuazione dell'ambito di trattamento consentito ai responsabili ed agli incaricati.

2.3. L'informativa

Ai sensi di quanto è prescritto dall'art. 15 del Regolamento di Ateneo, l'informativa di cui all'art. 13 del D.lgs. 196/2003, è a cura del responsabile del trattamento ed è resa all'interessato direttamente ovvero è effettuata con modalità idonee a garantire ampia diffusione della stessa.

L'informativa relativa al trattamento di dati sensibili e giudiziari deve contenere l'indicazione della normativa che prevede gli obblighi o i compiti in base alla quale il trattamento è effettuato. Inoltre, l'informativa relativa alla comunicazione e/o diffusione di dati personali deve essere sempre effettuata prima della trasmissione dei dati oggetto di trattamento.

In ogni caso, il responsabile è tenuto a conservare i documenti dai quali possa desumersi che l'informativa è stata resa in conformità alle disposizioni contenute nel Codice nonché nel Regolamento di Ateneo.

2.4. L'adozione delle misure minime di sicurezza

Al fine di garantire la sicurezza dei dati, il responsabile custodisce i dati seguendo le indicazioni che gli vengono fornite dal Titolare ed adottando ogni altra misura di sicurezza idonea a ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. A tal fine, impartisce le opportune istruzioni agli incaricati e vigila sul corretto svolgimento dei trattamenti di propria competenza.

Più specificatamente,il responsabile deve adottare, per lo svolgimento dei trattamenti di propria competenza, idonee soluzioni atte a garantire:

a) la disponibilità e l'utilizzo da parte degli incaricati di un idoneo sistema di autenticazione;
b) la attenta custodia delle credenziali di autenticazione degli incaricati;
c) la sicurezza del software e dell'hardware utilizzato dagli incaricati in termini di: manutenzione, installazione di prodotti di protezione dei sistemi, di prevenzione delle vulnerabilità e di correzione, strumenti e procedure per il salvataggio periodico dei dati.

2.5. Il Documento Programmatico sulla Sicurezza (DPS)

Ciascun responsabile di trattamento dei dati personali, responsabile di struttura didattica, di ricerca o di servizio (Polo, Facoltà, Dipartimento, Centro Interdipartimentale di Servizio o di Ricerca, Scuola di Specializzazione, Biblioteca, Centro di Ateneo, etc.) redige annualmente il Documento Programmatico sulla Sicurezza relativo al trattamento dei dati personali effettuati nel proprio ambito, eventualmente su schemi-tipo forniti dal Titolare ed avvalendosi dei contributi forniti dai responsabili del trattamento dei dati personali, ove presenti, di sotto-strutture afferenti alla struttura stessa.

Ciascun responsabile trasmette quindi al Titolare il DPS relativo al trattamento dei dati personali effettuato con strumenti elettronici nell'ambito della propria struttura, in modo tale da consentirne la allegazione al Documento Programmatico sulla Sicurezza dell'intero Ateneo, sottoposto dal Titolare al Consiglio di Amministrazione ed allegato al bilancio di previsione dell'Ateneo.

E' opportuno ricordare che la tenuta di un aggiornato DPS è tra le misure minime previste per i trattamenti automatizzati. Ai sensi dell'articolo 19 dell'allegato B del Codice, il DPS deve contenere:

- il censimento dei trattamenti di dati personali svolti (Reg. 19.1);
- l'analisi della distribuzione dei compiti e delle responsabilità (Reg. 19.2);
- l'analisi dei rischi incombenti sui dati (Reg. 19.3);
- la descrizione delle misure di garanzia adottate per l'integrità e la disponibilità dei dati, la protezione dei locali e delle aree (Reg. 19.4);
- la descrizione dei criteri e modalità per il ripristino dei dati a seguito di distruzione o danneggiamento, entro sette giorni nel caso di dati sensibili e giudiziari (Reg. 19.5);
- la previsione di interventi formativi a beneficio degli incaricati (Reg. 19.6);
- la descrizione dei criteri per l'affidamento di elaborazioni dati all'esterno della struttura del Titolare (Reg. 19.7);
- la descrizione dei criteri per la cifratura o la separazione di dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali dell'interessato (Reg. 19.8).

3. MISURE MINIME DI SICUREZZA IN FEDERICO II

3.1 Premessa

Le **"misure minime"** sono costituite, in accordo con quanto precedentemente detto, da quel complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali che l'Ateneo è tenuto ad adottare per ridurre al minimo i rischi di distruzione o di perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e che configurano il livello minimo di protezione richiesto dal Decreto Legislativo 196/2003 in materia di protezione dei dati personali.

Poiché il trattamento di dati personali può essere effettuato sia attraverso sistemi automatizzati sia attraverso supporti cartacei, è necessario distinguere tra:

1) Trattamenti automatizzati (effettuati con strumenti informatici e telematici)
2) Trattamenti non automatizzati (cartacei).

La presente guida, coerentemente con le misure minime definite nel Codice e con quanto prescritto nel Regolamento di Ateneo, contiene – tra l'altro – le istruzioni, le regole e le prassi a cui devono attenersi i responsabili e gli incaricati per la tutela dei dati personali trattati dall'Università degli Studi di Napoli Federico II.

Infine, è opportuno precisare che per tutto ciò che non è specificato nel presente manuale, il responsabile e l'incaricato osservano:

1) i principi contenuti nel D. Lgs. 196/2003 *Codice in materia di protezione dei dati personali*;
2) il *Regolamento di attuazione del Codice di Protezione dei dati personali utilizzati dall'Università*, adottato con D.R. n. 5073 del 30.12.2005;
3) Il *Regolamento di Ateneo in materia di Trattamento dei dati sensibili e giudiziari* adottato con D.R. n. 1163 del 22.03.2006.

3.2 Trattamenti automatizzati

Nell'ambito di tali trattamenti è necessario distinguere tra:

a) PC **non** collegati in rete;
b) PC collegati in rete ma **non** utilizzanti applicazioni informatiche centralizzate;
c) PC collegati in rete ed utilizzanti le applicazioni informatiche centralizzate.

3.2.1 Adempimenti di carattere generale previsti per tutte le tipologie di PC

3.2.1.1 Il sistema di autenticazione

L'autenticazione[2] fa riferimento alla capacità di un determinato sistema di consentire ad un utente autorizzato di accedere ai servizi ed alle informazioni cui ha legittimamente diritto e, contemporaneamente, di impedire qualunque tipo di accesso a chi, invece, non ha le autorizzazioni necessarie. L'applicazione di questo principio, ovviamente, comporta che il sistema debba essere in grado di memorizzare in modo sicuro le credenziali di ogni utente, di riconoscerlo all'atto della richiesta di un determinato servizio e di garantire che non possano avvenire manipolazioni delle richieste di accesso.

Tutti i PC devono essere accessibili attraverso l'utilizzo di un sistema di autenticazione, mediante l'utilizzo di password da inserire all'atto dell'accensione della macchina. I meccanismi da implementare dipendono dalla tipologia di PC (se collegato in rete locale, oppure no), dalle caratteristiche tecniche del PC e dalla disponibilità di idonee infrastrutture di servizio (ad esempio, la presenza di server di dominio). Tali aspetti saranno più diffusamente trattati nei prossimi paragrafi.

3.2.1.2 La segretezza e la custodia della password

Si sottolinea che l'attenta custodia della password di accensione va effettuata anche nell'interesse dello stesso utente al fine di non esporsi a dover rispondere di attività svolte da altri soggetti tramite il PC a lui assegnato.

Al fine di consentire l'uso del PC anche in caso di impedimento dell'incaricato che lo utilizza normalmente, questi dovrà consegnare al Responsabile del trattamento dei dati della struttura una busta chiusa contenente la propria password e provvedere a sostituirla in occasione dell'adozione di una nuova password.

Il responsabile del trattamento dei dati, in caso di impedimento temporaneo di un dipendente, qualora sia indispensabile utilizzare il PC a questi assegnato (anche per effettuare un intervento tecnico di manutenzione da parte del personale autorizzato, oppure perché utilizzato per uno specifico trattamento di dati personali), aprirà la busta contenente la relativa password e la fornirà ad altro dipendente per consentirgli l'utilizzo del detto PC. La busta, con l'indicazione della data della sua apertura, dovrà essere conservata a cura del Responsabile fino alla consegna della busta contenente la nuova password da parte del dipendente che è stato temporaneamente impedito.

Il Responsabile è tenuto, inoltre, a verificare la corretta applicazione delle disposizioni relative alla password di accensione del PC, riscontrando in particolare la sostituzione, ogni tre mesi, delle password (vale a dire delle buste contenenti le stesse).

3.2.1.3 Sicurezza del software e dell'hardware

Se nell'utilizzo del PC e/o dell'applicazione informatica a cui si è abilitati, viene rilevato un problema che può compromettere la sicurezza dei dati, l'incaricato ne dà immediata comunicazione al responsabile del trattamento che, a sua volta, provvede ad attivare la ditta o la struttura di Ateneo preposta alla manutenzione dei PC che analizzerà il problema segnalato ed adotterà tutte le misure tecniche necessarie a risolverlo. Nel caso dell'Amministrazione Centrale e degli uffici dei Poli, la struttura incaricata della manutenzione dei posti di lavoro è lo CSI che sarà attivato dal responsabile mediante Contact Center (al numero 081-676799).

[2] Definizione: un sistema di autenticazione è un dispositivo atto a stabilire e verificare in modo univoco, anche indiretto, l'identità dichiarata da un utente che vuole accedere al sistema, prima di ulteriori interazioni tra il sistema e l'utente.

All'utente è vietato installare programmi non attinenti le normali attività d'ufficio, né nuovi programmi necessari, né modificare le configurazioni hardware e software delle apparecchiature, senza il preventiva autorizzazione del proprio responsabile.

Gli utenti, con cadenza almeno mensile, verificano la presenza, sul sito ufficiale della Microsoft, di correzioni software per problemi di sicurezza, applicabili alla propria versione di sistema operativo. Se nel corso di tale verifica, effettuata attivando la funzione di Windows Update presente nei comandi principali del menù Start, si rileva la presenza di correzioni software per problemi di sicurezza (aggiornamenti critici), l'incaricato è tenuto a scaricare ed installare tali aggiornamenti sulla propria postazione di lavoro, seguendo le istruzioni riportate nel sito Microsoft. Tale adempimento è applicabile a tutti gli utenti le cui postazioni di lavoro sono collegate alla rete internet. Per i PC non in rete, l'aggiornamento dovrà essere eseguito da disco rimovibile.

Tutti gli incaricati evitano qualsiasi tipo di azione teso a superare le protezioni applicate ai sistemi e alle applicazioni. Gli interventi di installazione, configurazione e regolazione dei sistemi sono effettuabili solo la ditta o la struttura di Ateneo preposta alla manutenzione dei PC (nel caso dell'Amministrazione Centrale e degli uffici dei Poli, dallo CSI). A conclusione dell'intervento di manutenzione, il Responsabile del trattamento è tenuto comunque a verificare che il PC sia riportato nella situazione originaria per quanto riguarda le misure minime (password di accensione del PC, presenza del programma antivirus).

E' espressamente vietata qualsiasi azione volta a superare il blocco con password all'accensione del PC.

3.2.1.4 Protezione da virus informatici

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in essi presenti. Un virus informatico può danneggiare un PC, può modificare e/o cancellare i dati in esso contenuti, può compromettere la sicurezza e la riservatezza di un intero sistema informativo, può rendere indisponibile parti del sistema informativo, ivi compresa la rete di trasmissione dati.

I seguenti comportamenti inducono un aumento del livello di rischio di contaminazione da virus informatici:

1) installazione di software gratuito (freeware o shareware) prelevato da siti internet o allegato a riviste e/o libri;
2) scambio di file eseguibili allegati a messaggi di posta elettronica;
3) ricezione ed esecuzione di file eseguibili allegati a messaggi di posta elettronica;
4) collegamenti ad internet con esecuzione di file eseguibili, applets Java, ActiveX;
5) utilizzo della condivisione, senza password, di cartelle fra computer in rete;
6) utilizzo di floppy disk già utilizzati e la cui provenienza sia dubbia.

Al fine di evitare i problemi correlati alla diffusione di virus informatici, il responsabile e gli incaricati si attengono alle istruzioni di seguito riportate:

1) accertarsi che sul proprio computer sia sempre operativo uno dei programmi antivirus in uso presso l'Ateneo. Nel caso contrario segnalare immediatamente la situazione alla ditta o alla struttura di Ateneo preposta alla manutenzione dei PC (nel caso dell'Amministrazione Centrale, dallo CSI, tramite Contact Center);

2) aggiornare il programma antivirus, per i PC collegati in rete, automaticamente o su richiesta dell'utente, con cadenza almeno settimanale. Per i PC non collegati in rete l'aggiornamento del programma antivirus deve essere effettuato con cadenza almeno mensile;
3) accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati. Nel caso che il mittente del messaggio di posta elettronica dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati;
4) sottoporre a controllo, con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna e/o incerti prima di eseguire uno qualsiasi dei files in esso contenuti;
5) non condividere con altri computer il proprio disco rigido o una cartella senza password di protezione in lettura/scrittura;
6) proteggere in scrittura i propri floppy disk contenenti programmi eseguibili e/o files di dati;
7) limitare la trasmissione fra computer in rete di files eseguibili e di sistema;
8) non intraprendere azioni di modifica sui sistemi utilizzati a seguito di diffusione di messaggi e segnalazioni di virus informatici da qualsiasi fonte provengano. Le uniche azioni eventualmente necessarie sono comunicate esclusivamente dal Centro Servizi Informativi d'Ateneo (CSI);
9) non scaricare dalla rete internet programmi o files non inerenti l'attività dell'Ufficio o comunque sospetti;
10) distribuire preferibilmente documenti in formato elettronico avviene tramite formati standard, compatibili e possibilmente compressi (p.e. PDF).

Il Responsabile del trattamento dei dati della struttura è tenuto a verificare la corretta applicazione delle presenti disposizioni, accertando che tutti i PC dell'Ufficio siano dotati del programma antivirus. Nel caso riscontri la mancanza di tali protezioni minime, il responsabile è tenuto a far attivare il necessario intervento tecnico (nel caso dell'Amministrazione Centrale e degli uffici dei Poli, effettuando una chiamata al Contact Center dello CSI).

Nel caso in cui da parte del programma antivirus sia riscontrata la presenza di un virus informatico sul PC, l'Incaricato segue le istruzioni riportate sullo schermo dal programma e contestualmente avverte dell'evento il responsabile del trattamento dei dati. Quest'ultimo, dopo aver verificato che siano state rispettate le misure minime di protezione da virus informatici, provvede a segnalare l'evento per eventuali e successivi interventi tecnici alla ditta o alla struttura di Ateneo preposta alla manutenzione dei PC (nel caso dell'Amministrazione Centrale e degli uffici dei Poli, lo CSI, tramite Contact Center).

3.2.1.5 Salvataggio periodico dei dati

Per quanto garantire la disponibilità dei dati personali trattati con PC, a meno di meccanismi di salvataggio centralizzati (ma solo per i PC di tipologia b) e c)), il Responsabile è tenuto a verificare che, con cadenza almeno settimanale, tali dati siano archiviati su supporti di memorizzazione rimovibili (floppy disk, CDROM, DVD) e che tali supporti siano conservati in armadi o cassetti muniti di serratura, secondo quanto specificato al successivo paragrafo 3.3.

3.2.2 Adempimenti specifici previsti per il caso a) – PC non collegati in rete

Per i PC non collegati in rete, il meccanismo l'autenticazione deve essere necessariamente implementato in locale, sul PC.

Poiché i vecchi sistemi della famiglia Windows 9x (Windows 95, Windows 98, Windows 98 SE, Windows ME) non prevedono sistemi di autenticazione "nativi", la password di accensione deve essere in tal caso necessariamente di BIOS. La lunghezza minima della password è di 6 caratteri, o comunque del

massimo consentito dal BIOS del PC; la password BIOS deve essere modificabile dall'incaricato e variata almeno ogni sei mesi. Nel caso in cui sul PC risiedano dati sensibili o giudiziari, tale password deve essere modificata dall'incaricato almeno ogni tre mesi.

Di seguito, le regole valide per l'utilizzo della password BIOS:

Tabella 1 – Regole da implementare per l'utilizzo della password di BIOS

DESCRIZIONE	REGOLA
La password di BIOS può essere modificata dall'utente?	SI
Quale deve essere la durata della password di BIOS?	6 mesi oppure 3 mesi nel caso di trattamenti con dati sensibili o giudiziari
La password viene revocata in caso di mancato utilizzo?	NO
La password ha una lunghezza minima?	SI, 6 caratteri o comunque il massimo numero di caratteri consentiti dal BIOS del PC

I PC più recenti, (MAC OS, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista) sono invece dotati di sistemi di autenticazione ed autorizzazione completi che permettono non solo l'utilizzo di user-id e password, ma anche di credenziali di autenticazione "forte" quali token o device di riconoscimento biometrico. L'utilizzo dell'autenticazione "locale" non esclude l'adozione anche della password BIOS.

Di seguito, le regole valide per l'utilizzo della password locale del PC:

Tabella 2 – Regole da implementare per l'utilizzo della password locale del PC

DESCRIZIONE	REGOLA
La password locale del PC può essere modificata dall'utente?	SI
Quale deve essere la durata della password locale del PC?	6 mesi oppure 3 mesi nel caso di trattamenti con dati sensibili o giudiziari
La password viene revocata in caso di mancato utilizzo?	NO
La password deve avere una lunghezza minima?	SI, 8 caratteri

Per quanto attiene alle restanti misure minime di sicurezza, gli incaricati provvedono ad eseguire:
- con cadenza almeno mensile, da disco rimovibile, l'aggiornamento del sistema operativo presente sul proprio PC e del programma antivirus;
- con cadenza almeno settimanale, al salvataggio dei propri dati personali su supporti di memorizzazione rimovibili (floppy disk, CDROM, DVD) che devono essere conservati in armadi o cassetti muniti di serratura, secondo quanto specificato al successivo paragrafo 3.3;
- ad impostare la protezione mediante screen-saver con password.

E' opportuno evidenziare, infine, che i trattamenti eseguiti sui PC non collegati in rete devono essere autorizzati mediante modulo SICURDAT/A.

3.2.3 Adempimenti specifici previsti per il caso b) – PC collegati in rete ma non alle applicazioni centralizzate

Se il PC è collegato alla rete locale, l'autenticazione deve essere preferibilmente gestita da un sistema centralizzato di autenticazione. In tal caso, la password deve essere di lunghezza non inferiore a 8 caratteri o, comunque, al massimo numero di caratteri consentiti dal sistema di autenticazione utilizzato.

L'utilizzo di un sistema centralizzato di autenticazione, in generale, permette:

- la protezione e la gestione delle password (lunghezza minima, scadenza della password, rinnovo della password, cessazione dell'utenza, regole di composizione della password, ecc.) grazie ad un'unica procedura di accesso alle risorse di rete
- la profilazione utente grazie all'impostazione di privilegi per il controllo dell'accesso agli oggetti della directory e ai singoli elementi dati che li costituiscono
- la gestione della sicurezza anche dei sistemi client collegati
- la sicurezza nell'accesso ad Internet attraverso il supporto per i protocolli sicuri standard di Internet ed i meccanismi di autenticazione degli utenti quali Kerberos, PKI (Public Key Infrastructure) e LDAP (Lightweight Directory Access Protocol)
- la pre-impostazione centralizzata della protezione mediante screen-saver
- gestione della lista degli incaricati al trattamento dei dati in relazione al profilo di autorizzazione ed al conseguente ambito di trattamento consentito.

Sul mercato sono disponibili diverse ed interessanti soluzioni tecnologiche, alcune in ambiente Open Source, atte a garantire i requisiti di sicurezza precedentemente esposti. Sarà cura del responsabile individuare ed adottare la soluzione più idonea per la propria struttura.

Per l'**Amministrazione Centrale ed i Poli**, il sistema di autenticazione risiede su un server di dominio per il controllo di autorizzazione gestito dal Centro Servizi Informativi d'Ateneo (CSI). Le credenziali per l'autenticazione al dominio di rete del responsabile e degli incaricati sono richieste mediante il modulo SICURDAT/B. Inoltre, coerentemente con quanto prescritto dal Disciplinare Tecnico allegato al D.Lgs. 196/2003, la password di rete scade automaticamente ogni tre mesi e deve essere modificata dall'incaricato. Qualora, scaduto tale termine, la password non è modificata per ulteriori sei mesi, le credenziali sono disattivate. L'istanza di riattivazione va presentata, a cura del responsabile, mediante il modello SICURDAT/B. Infine, dopo cinque tentativi di connessione falliti, il codice identificativo (userid) è disabilitato. La richiesta di riabilitazione è effettuata dall'incaricato, tramite il Contact Center (al numero 081.676799) del CSI.

Di seguito, le regole da implementare su di un qualunque server di dominio ed attualmente impostate da CSI sui server d dominio che gestiscono l'autenticazione alla rete per i PC dell'Amministrazione Centrali ed i Poli. Tali regole si applicano anche per i PC di tipologia c):

Tabella 3 – Regole valide per userid e password per l'accesso alla rete (PC Amm. Centrale e Poli)

DESCRIZIONE	REGOLA
La password di rete può essere modificata dall'utente?	SI
Quale è la durata della password di rete?	3 mesi
Lo userid viene revocato in caso di mancato utilizzo?	SI, dopo sei mesi a partire dall'ultimo rinnovo password non eseguito
La password di rete ha una lunghezza minima?	SI, 8 caratteri o comunque il

	massimo numero di caratteri consentiti dal sistema di autenticazione utilizzato
Quanti sono i tentativi di prova di una password di rete prima che lo USERID sia disabilitato?	5

In generale, l'utilizzo della autenticazione tramite il server di dominio non esclude l'utilizzo della password BIOS.

Per quanto riguarda il salvataggio dei dati personali residenti sulle postazioni di lavoro **dell'Amministrazione Centrale e degli uffici dei Poli**, a ciascun incaricato è assegnato un codice identificativo personale ed una password di rete mediante i quali l'incaricato può accedere ed utilizzare le risorse di rete. Ciascun incaricato in possesso di una credenziale di autenticazione alla rete ha accesso, in lettura e scrittura, ad una cartella comune dedicata al proprio ufficio e ad una cartella personale, entrambe di capacità pari a 100 MB, in cui deve salvare, almeno con frequenza settimanale, i dati personali contenuti sul proprio PC. Le cartelle risiedono su server gestiti da CSI, in modo tale da garantire integrità, disponibilità e riservatezza dei dati registrati. L'accesso (in lettura, in scrittura, in lettura/scrittura) alle sotto-cartelle contenute nella cartella comune viene consentita agli incaricati afferenti all'intero Ufficio, oppure a gruppi nell'ambito dell'Ufficio, oppure a singoli dipendenti, sulla base di specifiche richieste concordate tra il Responsabile ed il C.S.I.. In assenza di richieste, la regola base adottata dal C.S.I. è di consentire, per ciascun Ufficio, l'accesso in lettura/scrittura a tutti gli incaricati dell'Ufficio stesso.

Richieste di accessibilità ad ulteriori risorse di rete sono specificate ed autorizzate mediante il modulo SICURDAT/B.

Il responsabile è tenuto a verificare che siano rispettate le indicazioni precedentemente riportate da parte di ciascun incaricato.

In casi eccezionali, anche per i PC collegati in rete, il salvataggio dei dati può essere effettuato su supporti di memorizzazione rimovibili (floppy disk, CDROM, DVD) che devono essere conservati in armadi o cassetti muniti di serratura, secondo quanto specificato al successivo paragrafo 3.3.

3.2.4 Adempimenti specifici previsti per il caso c) – PC collegati in rete ed alle applicazioni centralizzate

A tali PC si applicano le norme previste per il caso b), con l'aggiunta delle prescrizioni di seguito riportate.

Ad ogni utente delle applicazioni informatiche centralizzate, per ciascuna applicazione, sono associati un codice identificativo personale, una password ed eventualmente un profilo di abilitazione.

Il responsabile del trattamento dei dati dovrà individuare tassativamente per iscritto, compilando l'apposito modulo SICURDAT/B, gli incaricati dei trattamenti informatizzati mediante procedure centralizzate. Tale incarico conferisce, implicitamente, anche l'autorizzazione all'utilizzo della corrispondente procedura informatica. I permessi dell'utente saranno tali da consentire le operazioni di trattamento richieste nel modello SICURDAT/B. I profili di abilitazione di ciascun incaricato sono tenuti ed aggiornati dal CSI.

Di seguito, infine, si riportano alcune informazioni utili sulla gestione del codice identificativo personale (userid) e della password per l'accesso alle applicazioni informatiche centralizzate.

Ad ogni utente delle applicazioni informatiche centralizzate è associato un codice identificativo personale (userid), una password ed un profilo di abilitazione. Alcune applicazioni prevedono due diversi livelli di identificazione: uno di *sistema* ed uno *applicativo*. Le applicazioni informatiche riportate nel SICURDAT/B che prevedono un doppio livello di identificazione sono: la procedura di Gestione del Personale - con inclusa la gestione dei Dottorati di Ricerca (CSA), la procedura per la gestione della Contabilità Integrata d'Ateneo (CIA) e la procedura Gestione Ticket (GTIK). Solo per queste procedure, l'utente deve identificarsi preliminarmente verso il *sistema*, attraverso la maschera di collegamento al CSI e, successivamente, identificarsi verso *l'applicazione.*

Le altre applicazioni informatiche prevedono un solo livello di identificazione dell'utente. Queste ultime sono: la procedura di Gestione della Rilevazione delle Presenze (SIRP), la procedura Segreteria Studenti (GEDAS), la procedura Organi Collegiali (SIOC), la procedura Protocollo (E-Grammata), la procedura di valutazione comparativa (VALCOM), la procedura per la gestione delle utenze e del traffico telefonico (GUTTEL), la procedura INPDAP per la gestione dei dati di Previdenza ed Assistenza dei dipendenti e l'applicazione per le Biblioteche Digitali.

A seconda del tipo di applicazione informatica utilizzata, le regole applicabili allo userid e alla password, sono diverse. In particolare il quadro delle regole attualmente in essere, è riportato nella tabella seguente.

Tabella 4 – Regole valide per userid e password delle applicazioni informatiche centralizzate

	SIRP	CSA	GEDAS	SIOC	GUTTEL	E-GRAMMATA	CIA	GTIK	VALCOM	BIBL. DIGITALI
Livelli di identificazione	1	2	1	1	1	1	2	2	1	1
La password può essere modificata dall'utente?	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI
Quale è la durata della password ?	30 gg.	3 mesi	30 gg.		6 mesi		3 mesi	30 gg.	60gg.	
Lo userid viene revocato in caso di mancato utilizzo?	NO	NO	NO	NO	NO	NO	NO	SI, dopo 45 gg.	NO	NO
La password ha una lunghezza minima?	NO	SI (8)	SI (6)	SI (3)	SI (8)	SI (8)	SI (8)	SI (6)	NO	NO
Tentativi di prova della password prima che lo USERID sia disabilitato		5 userid sist.			3		5 userid sist.	5	3	

I codici di abilitazione disponibili per le diverse applicazioni sono riportati nel modello SICURDAT/B.

3.2.5 Utilizzo della rete internet

Il sistema informativo dell'Ateneo ed i dati in esso contenuti possono subire gravi danneggiamenti per effetto di un utilizzo improprio della connessione alla rete internet; inoltre, attraverso tale rete possono penetrare nel sistema virus informatici ed utenti non autorizzati. Allo scopo di evitare questi pericoli, gli Incaricati che dispongono di PC collegati in rete (caso b) e c)), curano l'applicazione delle seguenti regole:

1) utilizzano la connessione ad internet esclusivamente per lo svolgimento dei compiti istituzionali dell'Ufficio;
2) si astengono da un uso di internet illegale o non etico;
3) rispettano l'obbligo di non collegarsi a siti con materiale illegale e/o inappropriato;
4) si astengono dall'inviare, ricevere o mostrare testi o immagini che possono essere offensivi per le persone presenti;
5) rispettano i diritti di proprietà intellettuale facendo solo copie autorizzate di programmi o dati coperti da copyright;
6) non danneggiano né alterano il Setup o la configurazione software della propria postazione di lavoro, evitando inoltre di installare prodotti software non licenziati e/o non certificati a corredo della postazione per la specifica destinazione d'uso;
7) rispettano la privacy delle altre persone non facendosi passare per un altro utente della rete, non tentando di modificare o accedere a file, password o dati che appartengono ad altri, non cercando di disattivare il controllo di autorizzazione all'accesso a qualunque sistema o rete di computer;
8) non diffondono messaggi di posta elettronica di provenienza dubbia, non partecipano a sequenze di invii di messaggi (catene di S. Antonio) e non inoltrano o diffondono messaggi che annunciano nuovi virus;
9) sono responsabili dell'uso della casella di posta elettronica istituzionale loro assegnata, non utilizzano le caselle di posta elettronica istituzionali per fini privati o personali, limitano allo stretto indispensabile l'invio di messaggi di posta elettronica con allegati, scegliendo, ove necessario, il formato degli allegati che occupa meno spazio;
10) non utilizzano servizi di comunicazione e condivisione files che esulino dalle ordinarie funzioni di browsing internet (http), posta elettronica e trasferimento files;
11) sono a conoscenza degli articoli del Codice Penale 615 ter – "*Accesso abusivo ad un sistema informatico o telematico*", 615 quater – "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*", 615 quinquies – "*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*", nonché del Decreto legge 22 marzo 2004 n.72 convertito in legge con modificazioni dalla Legge 21 maggio 2004 n.128, (Legge Urbani) che sanziona la condivisione e/o la fruizione di file relativi ad un'opera cinematografica o assimilata protetta dal diritto d'autore.

3.2.6 Utilizzo di supporti rimovibili

E' sconsigliata la scrittura di dati sensibili e giudiziari su supporti rimovibili (floppies, DVD, dispositivi USB, CDROM, CD riscrivibili, etc.). Qualora se ne ravvisi l'indispensabilità, è necessario ridurre al minimo la permanenza di tali dati sul dispositivo utilizzato e, al termine del trattamento effettuato, provvedere:

- alla loro cancellazione mediante tecniche che li rendano non intelligibili e ricostruibili, se riutilizzati per differenti trattamenti,
  oppure,
- alla loro distruzione,
  oppure,

- alla loro conservazione secondo quanto prescritto al successivo punto.

3.3 Trattamenti non automatizzati

L'autorizzazione al trattamento di dati personali, sensibili e giudiziari effettuato senza l'ausilio di strumenti elettronici è richiesta dal responsabile mediante il modello SICURDAT/A.

L'allegato A**,** in aggiunta alle disposizioni di carattere generale valide per tutti i trattamenti non automatizzati di seguito riportate, contiene le "DISPOSIZIONI RELATIVE AL PROTOCOLLO E AGLI ARCHIVI", valide per i Poli e, soprattutto, per l'Amministrazione Centrale.

3.3.7 Dati personali non sensibili né giudiziari

I responsabili del trattamento dei dati provvedono ad attuare le misure di protezione tese ad evitare l'accesso a persone non autorizzate ad archivi contenenti dati personali. Tra le misure utilizzabili si individuano le seguenti misure minime:

1) la sistemazione degli archivi e dei fascicoli in locali protetti da serrature;
2) l'utilizzo di mobili muniti di serrature per la raccolta e la conservazione dei fascicoli e dei documenti;
3) l'utilizzo di armadi ignifughi per la conservazione dei supporti informatici sui quali siano presenti copie di archivi contenenti dati personali.

Le misure di protezione di cui ai punti 1) e 2) sono **obbligatorie**, la misura di protezione individuata al punto 3) è da considerarsi opzionale.

Gli incaricati del trattamento dei dati evitano comportamenti che possano pregiudicare la riservatezza dei dati. Per esigenze specifiche chiedono indicazioni e direttive al responsabile del trattamento dei dati.

3.3.8 Dati sensibili e giudiziari

E' obbligatorio conservare i dati solo in contenitori appositamente individuati, evitando dunque di collocare i documenti o i supporti informatici che li contengono in luoghi diversi, o di lasciarli fuori dagli stessi. In particolare non è consentito lasciare le pratiche contenenti dati sensibili sulla scrivania o comunque a portata di mano, se non per il tempo necessario all'effettivo utilizzo, al termine del quale i documenti vanno comunque riposti.

Ogni incaricato deve riporre i documenti o i supporti informatici contenenti dati sensibili o giudiziari negli appositi contenitori o scaffali al termine delle operazioni affidate e comunque a fine giornata. In ogni caso di allontanamento dal proprio posto di lavoro, i documenti devono essere riposti o negli armadi o nei cassetti e chiusi a chiave.

I dati idonei a rivelare lo stato di salute o la vita sessuale devono essere conservati separatamente dagli altri dati.

3.3.9 I PIN degli studenti

Fra i dati personali vanno annoverati i PIN degli studenti attraverso la cui conoscenza (associata alla conoscenza del numero di matricola) è possibile accedere a tutti i dati dello studente, ivi compresi quelli relativi ad eventuali situazioni di handicap e quindi sensibili.

E', pertanto, opportuno che gli elenchi contenenti i PIN, forniti alle Segreterie studenti dallo CSI, vengano utilizzati e conservati con tutte le cautele del caso che i responsabili provvederanno ad individuare.

3.4 Videosorveglianza

Il Garante per la protezione dei dati personali, con apposito provvedimento, ha fornito le indicazioni da seguire ai fini di una corretta gestione dei sistemi di videosorveglianza. In attuazione di detto provvedimento, coerentemente con quanto disposto nel citato "Regolamento d'Ateneo di attuazione del codice di protezione dei dati personali", si riportano di seguito le disposizioni da osservare:

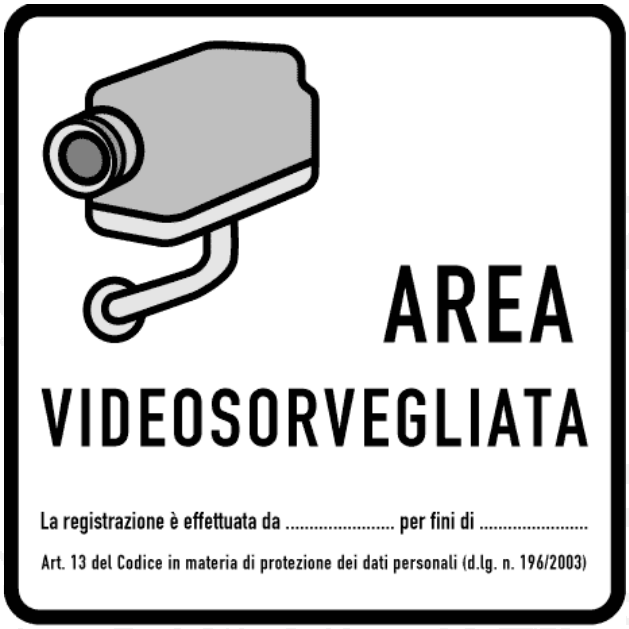
- il Responsabile dovrà verificare che i sistemi di video sorveglianza non costituiscano mezzo di controllo a distanza dei lavoratori, in ossequio alla disposizione di cui all'art. 4 della legge 300/1970;
- il Responsabile dovrà, inoltre, garantire che le immagini riprese siano visualizzate soltanto dagli incaricati (dipendenti dell'Ateneo o soggetti esterni) appositamente nominati, esclusivamente per finalità di tutela dei beni e delle persone che si trovano nelle Sedi sorvegliate. Dovrà garantire, altresì, che le immagini registrate siano conservate per un periodo non superiore alle 24 ore. La visualizzazione delle immagini registrate dovrà avvenire esclusivamente nel caso in cui si verifichi un illecito o in relazione ad indagini dell'autorità giudiziaria o di polizia;
- il responsabile dovrà, infine, rendere alle persone che possono essere riprese idonea informativa, ai sensi dell'art. 13 del Codice, circa la presenza degli impianti, curandosi di affiggere appositi cartelli nei luoghi ripresi dalle telecamere. In particolare, potrà utilizzare in aree esterne il modello semplificato di informativa "minima" elaborato dal Garante per la Protezione dei Dati Personali, di seguito riportato in fac-simile. Nelle restanti aree, l'informativa - più dettagliata - dovrà indicare le finalità e le modalità del trattamento, precisando le modalità di conservazione e visualizzazione delle immagini e i nominativi dei soggetti autorizzati a tali operazioni, secondo quanto di seguito indicato:

INFORMATIVA
(ai sensi dell'art. 13 del D.Lgs 196/2003)

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali si informa che in questo locale è presente un impianto di videosorveglianza, istallato per ragioni di sicurezza e di tutela dei beni che si trovano in questo Edificio.
Le immagini riprese possono essere visualizzate soltanto dagli Incaricati del servizio di custodia e vigilanza afferenti alla Amministrazione Centrale dell'Università degli Studi di Napoli Federico II, esclusivamente per le finalità innanzi indicate.
Le immagini registrate vengono conservate per un periodo non superiore alle 24 ore. Esse possono essere visualizzate dal Responsabile e dagli Incaricati del trattamento esclusivamente nel caso in cui si verifichi un illecito o in relazione ad indagini dell'autorità giudiziaria o di polizia.
Titolare del trattamento è l'Università degli Studi di Napoli Federico II.
Il Responsabile del trattamento è Responsabile dell'Ufficio _____.

MODELLO SEMPLIFICATO INFORMATIVA PER LA VIDEOSORVEGLIANZA

(contenuto nel "Provvedimento generale sulla videosorveglianza" del Garante per la Protezione di Dati Personali, pubblicato il 29 aprile 2004)



4. RACCOMANDAZIONI GENERALI

4.1 Distanza di cortesia

L'udienza degli utenti va organizzata in modo da evitare che altri, dipendenti o non dipendenti, possano, anche involontariamente, ascoltare i colloqui che ciascun utente intrattiene con il personale addetto a recepire le relative istanze. Deve, cioè, essere garantita la *c.d. distanza di cortesia* nelle ipotesi in cui vengano in rilievo dati personali dell'interessato.

4.2 Linee guida per il corretto utilizzo di userid e password

La sicurezza logica si realizza assicurando che tutti gli accessi ai diversi componenti del sistema informativo dell'Ateneo avvengano esclusivamente secondo modalità prestabilite. Per tale motivo, ogni qual volta si rende necessario l'utilizzo di una risorsa informatica, deve essere presente un meccanismo che costringa l'utente (responsabile o incaricato privacy) ad autenticarsi, ossia a dimostrare la propria identità, mediante tipicamente l'utilizzo di un codice identificativo personale (userid) ed una parola chiave (password).

Tutti gli utenti rispettano le seguenti disposizioni:

A) L'utente è responsabile della corretta tenuta della password di accensione del PC che gli è stato assegnato e delle eventuali password di accesso alla rete e alle applicazioni;
B) L'utente a cui è stata assegnata una userid per l'accesso alla rete e/o per l'utilizzo di applicazioni informatiche centralizzate, è responsabile di tutto quanto accade a seguito di transazioni ed elaborazioni abilitate dal proprio codice identificativo personale. Per le applicazioni informatiche centralizzate, tale responsabilità deve essere riferita ai privilegi associati al suo profilo di abilitazione;
C) L'utente cambia le proprie password secondo le disposizioni riportate nel presente manuale;
D) L'utente gestisce le proprie password secondo le disposizioni riportate nel presente manuale;
E) L'utente attiva tutte le misure in suo potere per evitare che terzi abbiano accesso al suo PC mentre si allontana durante una sessione di lavoro. A tal fine esce sempre dall'applicazione in uso (logoff) o eventualmente blocca il PC con uno screen saver protetto da password;
F) L'utente non comunica a nessun altro utente le proprie password.

In generale, vi sono diverse categorie di password, ognuna con il proprio ruolo preciso:

a) **la password di accensione del PC** (password di BIOS o locale) impedisce l'utilizzo improprio della propria postazione di lavoro, quando per un qualsiasi motivo non ci si trova in ufficio;
b) **la password di rete** impedisce che l'eventuale accesso non autorizzato ad un PC renda disponibili le risorse dell'ufficio (stampanti, cartelle condivise);
c) **la password delle applicazioni informatiche centralizzate** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato;
d) **la password di protezione delle risorse (cartelle) condivise** impedisce l'accesso a tali risorse da parte di utenti non autorizzati i cui PC siano collegati sulla stessa rete locale ed impedisce la propagazione di virus informatici nella rete locale;

e) **la password della casella di posta elettronica istituzionale** impedisce che i messaggi di posta elettronica indirizzati ad un utente possano essere letti da utenti non autorizzati;
f) **la password del salva schermo** impedisce che un'assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro in corso e/o di accedere ai documenti residenti sulla postazione di lavoro.

La gestione delle password indicate sono disciplinata dal **Disciplinare tecnico in materia di misure minime di sicurezza - D. Lgs. 196/03, Allegato B** (regole da 1 a 11): in sintesi, esse hanno una lunghezza non inferiore ad 8 caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo; queste password sono modificate dall' Incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari, la password deve essere modificata almeno ogni tre mesi. Le credenziali sono inoltre disattivate dopo sei mesi di mancato utilizzo e sono revocate nel caso di perdita delle qualità che consente all'utente l'accesso ai dati personali.

Le password di cui ai punti e) ed f) rappresentano un ulteriore livello di protezione il cui impiego è lasciato alla discrezione dell'utente della postazione di lavoro.

Nella gestione delle password è necessario attenersi alle indicazioni di seguito riportate.

Cosa NON fare:

1) NON comunicare a NESSUNO le proprie password, qualunque sia il mezzo che viene utilizzato per inoltrare la richiesta (telefono, messaggio di posta elettronica, ecc.). Ricordare che NESSUNO è autorizzato a richiedere le password, nemmeno il personale tecnico di supporto o gli addetti alla manutenzione delle postazioni di lavoro, e che lo scopo principale per cui sono utilizzate le password è di assicurare che nessun altro possa utilizzare le risorse a cui si è abilitati;
2) NON scrivere le password su supporti che possano essere trovati facilmente e/o soprattutto in prossimità della postazione di lavoro utilizzata;
3) NON scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Esistono programmi che permettono di provare come password tutte quelle contenute in dizionari elettronici estremamente ampi, in termini di numero di lemmi, e in diverse lingue, scritte sia in senso normale che in senso inverso;
4) NON usare come password il nome utente o parole che possano essere facilmente riconducibili all'identità dell'utente, come, ad esempio, il codice fiscale, il nome del coniuge, il nome dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della strada in cui si abita, il nome della squadra di calcio per cui si tifa, ecc.;
5) NON usare come password parole ottenute da una combinazione di tasti vicini sulla tastiera o sequenze di caratteri (esempio: qwerty, asdfgh, 123321, aaabbb, ecc.);
6) NON usare la STESSA password per le diverse tipologie di password prima individuate;
7) NON rendere note password vecchie e non più in uso, in quanto da questi dati è possibile ricavare informazioni su ciclicità e/o regole empiriche e personali che l'utente utilizza per generare le proprie password.

Cosa FARE:

1) Cambiare le password frequentemente ricordando che il limite massimo di validità di una password stabilito dalle presenti misure minime è di 6 mesi;
2) Utilizzare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione;

3) Nella digitazione delle password assicurarsi che non ci sia nessuno che osservi ciò che si digita sulla tastiera del PC;
4) Utilizzare password distinte per le diverse tipologie di password prima descritte.

4.3 Come scegliere le password

La scelta della password da parte dell'utente deve essere oculata, in quanto il modo più semplice e più utilizzato per realizzare un accesso illecito ad un sistema e/o ad un applicazione, consiste nell'ottenere le credenziali identificative di un utente autorizzato, ossia la sua coppia userid e password. La scelta, quindi, di password "forti" rappresenta un aspetto essenziale della sicurezza informatica.

Le password migliori sono quelle facili da ricordare ma, allo stesso tempo, difficili da individuare. Questo genere di password può essere ottenuto, ad esempio, comprimendo frasi lunghe in pochi caratteri presenti nella frase, utilizzando anche segni di interpunzione e caratteri maiuscoli e minuscoli. La frase "Nel 1969 l'uomo è andato sulla luna" può, ad esempio, fornire tra le tante possibilità la seguente "N69UèAsL".

Accanto a questa tecnica, per ottenere password ancora più "forti", si possono sostituire le lettere risultanti dalla compressione della frase, con cifre o caratteri che assomiglino alle lettere; ad esempio la frase "Questo può essere un modo per ricordare la password" diventa "Qp&1mpRP".

Un altro modo per ottenere password "forti" consiste nel combinare date o numeri che si ricordano facilmente con pezzi di parole che sono in qualche modo abituali e quindi semplici da ricordare; ad esempio la combinazione "felice1983", che utilizzata direttamente potrebbe essere una password "debole" (combinazione del nome del figlio e della data di nascita), può diventare una password migliore in questo modo "FeLi83ce", o una password "forte" così "F&Li83cE".

N.B. Non utilizzare come password gli esempi riportati nel presente manuale.

Allegato A - DISPOSIZIONI RELATIVE AL PROTOCOLLO ED AGLI ARCHIVI

A.1 Il Protocollo

Il protocollo rappresenta, ai fini della tutela della riservatezza, della disponibilità e della integrità, un settore particolarmente delicato, considerato che vi transitano tutti i documenti dell'Ateneo sia in entrata che in uscita. Ciò implica che gli addetti agli Uffici Protocollo di ciascuna struttura (Unità Organizzativa Responsabile) dell'Ateneo, anche se per il solo transito di documenti, gestiscono quasi la totalità delle informazioni che vengono trattate dall'amministrazione.

Risulta dunque indispensabile che essi siano particolarmente attenti, nello svolgimento delle attività di competenza, alla problematica in oggetto.

Si ribadiscono pertanto tutte le disposizioni dettate in precedenza per il trattamento dei dati personali (sia automatizzati che non automatizzati), sottolineando alcuni aspetti ulteriori che per il settore in argomento assumono particolare rilievo:

- l'accesso all'ufficio va costantemente controllato;
- gli addetti di altre strutture devono effettuare le operazioni di prelievo e consegna di documenti nel locale d'ingresso;
- non è consentito intrattenersi presso i locali dell'ufficio se non per il tempo strettamente necessario alla consegna o al prelievo;
- l'ufficio disporrà affinché una unità di personale sia addetta al ricevimento dei documenti, evitando l'accesso all'ufficio da parte di personale di altre strutture, quando ciò non sia necessario;
- ciascun addetto al protocollo deve avere accesso ai soli documenti indispensabili allo svolgimento dei compiti assegnati.

A.2 La tenuta dell'Archivio presso l'Amministrazione Centrale

Ad integrazione e parziale modifica del precedente Ordine di Servizio n.47 del 31.01.02006, con Ordine di Servizio n.403 del 07.12.2007 si è provveduto a fornire ulteriori indicazioni in tema di sicurezza dei locali appositamente destinati all'archivio del Palazzo degli Uffici.
In particolare, la custodia delle chiavi dell'archivio è stata affidata ad una unità di personale afferente all'Ufficio Servizi Generali. La predetta unità di personale tiene, altresì, il registro degli accessi sul quale devono essere annotate le seguenti informazioni: l'ora d'ingresso all'archivio e quella d'uscita, il nominativo della persona che accede ai locali e la tipologia di attività. Sono inoltre individuate in modo puntuale i nominativi dei sostituti (addetti alla custodia del Palazzo degli Uffici) che garantiscono l'accesso allo archivio nelle ore successive all'orario di servizio dell'incaricato.

A.3 La tenuta dell'Archivio presso i Poli

Presso ciascun Polo sono individuati dei locali chiusi a chiave per l'archiviazione dei documenti e dei fascicoli. La custodia ed il controllo sul prelievo e ricollocazione della documentazione di volta in volta occorrente agli uffici del Polo è formalmente affidata, dal Direttore, ad un ufficio del Polo.

Il personale addetto al controllo dell'archivio dovrà consentire l'accesso all'archivio esclusivamente al personale munito di autorizzazione firmata dal responsabile dell'ufficio richiedente ed opportunamente esibita. Tale autorizzazione sarà debitamente firmata dall'incaricato dell'ufficio richiedente, per ricevuta. La consegna della documentazione sarà, in modo del tutto analogo, accompagnata da una nota firmata dall'ufficio richiedente e controfirmata, per accettazione, da parte dell'ufficio preposto alla tenuta dell'archivio.