UNIVERSITÀ DEGLI STUDI DI MILANO

BREVE COMPENDIO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

PREMESSA

La presente trattazione, che si allega all'atto di nomina a "**INCARICATO DEL TRATTAMENTO**", riassume i principi fondamentali della normativa vigente in materia di tutela dei dati personali, per favorire la conoscenza e la corretta applicazione di tale normativa da parte di tutti i soggetti incaricati, nell'ambito dell'Ateneo, del trattamento di dati personali.

Il compendio, in particolare, comprende:

- una panoramica sulla normativa in vigore (legislazione statale e universitaria in materia di privacy);
- una raccolta di definizioni, riguardanti i termini "tecnici" maggiormente ricorrenti;
- la descrizione dei soggetti che partecipano al trattamento e delle rispettive competenze;
- un sunto delle principali regole per un corretto trattamento dei dati.

Sul sito d'Ateneo è stata predisposta una sezione dedicata alla Privacy (http://www.unimi.it/aree_protette/5866.htm), dove si possono trovare ulteriori informazioni e documenti utili per l'applicazione della normativa in materia di protezione dei dati personali.

IL QUADRO NORMATIVO

1. Normativa nazionale: Codice e Allegati

A decorrere dal 1 gennaio 2004, è entrato in vigore il *d. lgs. n. 196/2003* (*Codice in materia di protezione dei dati personali*, di seguito denominato "*Codice*" o "*Testo Unico*"), che ha riunito in un unico corpo le disposizioni previgenti, introducendo altresì importanti innovazioni (il testo è reperibile alla pagina sopraindicata del sito Internet d'Ateneo).

Strutturalmente il Codice è articolato in 3 parti:

- la prima (artt. 1/45) dedicata ai principi e alle regole generali per il trattamento dei dati;
- la seconda (artt. 46/140) riguardante i trattamenti effettuati nell'ambito di settori specifici, tra i quali rivestono particolare interesse, per quanto di competenza dell'Università, i "trattamenti in ambito pubblico" (artt. 59/74) e il "trattamento per scopi storici, statistici o scientifici" (artt. 97/110);
- la terza concernente gli strumenti di tutela e le sanzioni amministrative e penali.

Otto allegati completano il Codice.
Di particolare importanza per l'Ateneo, si segnalano:
-il *"Codice Deontologico e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (Allegato A4)*", che si applica a tutti i trattamenti posti

in essere per le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

-*l'Allegato B - disciplinare tecnico in materia di misure minime di sicurezza*, che descrive le misure minime che è indispensabile adottare per garantire la sicurezza dei dati nell'ambito dei trattamenti effettuati sia mediante strumenti elettronici sia senza l'ausilio di tali strumenti.

La disciplina codicistica è finalizzata a garantire, in un'ottica di ampia protezione dei dati personali, che il trattamento dei medesimi si svolga solo per il raggiungimento delle finalità istituzionali (principio di necessità), nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

2. Provvedimenti del Garante Privacy.

Il Garante per la protezione dei dati personali, autorità istituita con la L. 675/96, attualmente disciplinata dagli artt. 153 e 154 del Codice, ha emanato negli anni diversi Provvedimenti Generali in materie specifiche, tra i quali si segnalano:

- il Provvedimento Generale del 27/11/2008 in materia di *"Amministratori di sistema"* ;
- il Provvedimento Generale dell'08/04/2010 in materia di *"Videosorveglianza"* .

3. Normativa universitaria.

- In data 4/12/2004, l'Università degli Studi di Milano ha adottato il *Regolamento d'Ateneo in materia di protezione dei dati personali* (di seguito Regolamento), con cui sono state recepite le disposizioni applicabili all'attività svolta in ambito universitario.

In seguito ad alcuni interventi legislativi cha hanno modificato la materia, al Regolamento d'Ateneo sono state apportate alcune modifiche con Decreto Rettorale n. 0288433 del 13/12/2013.

- In data 28/03/2006 il Consiglio di Amministrazione dell'Università ha approvato il *Regolamento Dati Sensibili e Giudiziari* secondo lo schema-tipo approvato dal Garante in data 17/12/2005.

DEFINIZIONI

Dati personali: per dati personali si intende qualunque informazione relativa a persona fisica, identificata o identificabile (nome, cognome, data di nascita, codice fiscale, partita IVA, fotografie, ma anche i dati relativi al traffico telefonico, all'uso della posta elettronica e al collegamento in rete – c.d. file di log). I dati non personali sono detti anonimi, in quanto, sin dall'origine o in seguito a trattamento, non possono essere associati ad un interessato identificato o identificabile.

Dati sensibili: sono 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 o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari: sono i dati personali idonei a rivelare provvedimenti del giudice penale per i quali è prevista l'iscrizione nel casellario giudiziale, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Banca di dati: è un complesso organizzato (archivio) di dati personali, di tipo cartaceo o elettronico.

Interessato: è la persona fisica, cui si riferiscono i dati personali.

Trattamento: si intende, per trattamento, qualunque operazione effettuata, con o senza l'ausilio di strumenti elettronici, su dati (raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione).

Comunicazione: operazione consistente nel dare conoscenza di dati personali a uno o più soggetti determinati diversi dall'interessato (e ad esclusione del Titolare, del Responsabile e degli Incaricati del trattamento).

Diffusione: operazione consistente nel dare conoscenza dei dati personali a soggetti indeterminati.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Misure minime di sicurezza: si tratta del complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione in relazione ai rischi cui si trovano esposti i dati personali.

Autenticazione informatica: è l'insieme degli strumenti elettronici e delle procedure diretti alla verifica dell'identità del soggetto che intende accedere ai dati personali.

Credenziali di autenticazione: sono i dati e i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati (ad esempio, password), utilizzati per l'autenticazione informatica.

User ID: codice identificativo personale formato da lettere e/o numeri, utilizzato in associazione ad una password per l'autenticazione informatica.

Password: parola chiave associata a una persona e da questa conosciuta, costituita da una sequenza di caratteri o altri dati in forma elettronica, utilizzata per l'autenticazione informatica.

Profilo di autorizzazione: è l'ambito dei dati ai quali un incaricato può accedere e dei trattamenti che gli è consentito compiere; possono essere previsti, in ogni caso

anteriormente all'inizio del trattamento, profili personalizzati o comuni a specifiche categorie di Incaricati.

Sistema di autorizzazione: è l'insieme degli strumenti e delle procedure che abilitano l'Incaricato ad accedere ai dati e alle tipologie di trattamento, in funzione del proprio profilo di autorizzazione.

Scopi storici: le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato.

Scopi statistici: le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi.

Scopi scientifici: le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Garante: è l'autorità istituita dalla legge a garanzia del rispetto delle norme in materia di protezione dei dati personali. È un organo collegiale composto da quattro componenti che, operando in piena autonomia e con indipendenza di giudizio, esercita funzioni di controllo, esprime pareri, riceve le segnalazioni e i ricorsi da parte degli interessati in relazione a presunte violazioni della normativa, emette al riguardo eventuali provvedimenti nei confronti del Titolare / Responsabile.

I SOGGETTI CHE PARTECIPANO AL TRATTAMENTO

Titolare: è il soggetto cui competono le decisioni in ordine alle modalità e alle finalità del trattamento dei dati personali.

Per quanto riguarda i dati gestiti dall'Università degli Studi di Milano, Titolare è l'Università stessa, nella persona del Rettore.

Responsabile: è il soggetto preposto dal Titolare al trattamento dei dati; è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.

Nell'ambito di questo Ateneo il Titolare ha provveduto a nominare un Responsabile del trattamento per ciascuna struttura (Dipartimenti, Divisioni Amministrative …), individuandolo di norma nel Responsabile della struttura stessa (Direttore di Dipartimento, Capo Divisione …); è fatta salva la possibilità per quest'ultimo di designare altro soggetto che risponda ai requisiti prescritti.

Incaricato: è la persona fisica che compie materialmente le operazioni di trattamento dei dati, attenendosi alle istruzioni impartite dal Titolare e dal Responsabile.

In Ateneo ciascun Responsabile, nell'ambito della propria struttura, nomina Incaricato chiunque debba compiere, per lo svolgimento delle proprie funzioni, operazioni di trattamento di dati personali.

Custode delle password (punto 10 All. B "Disciplinare Tecnico" del Codice): è l'Incaricato che, nell'ambito di ciascuna struttura, viene preposto dal Responsabile alla custodia delle password.

Il custode non è a conoscenza delle password degli altri Incaricati – custodite in busta chiusa controfirmata contenente il modulo utilizzato dal singolo Incaricato per indicare la parola chiave scelta - ma si limita a conservarle con le dovute cautele.

In caso di assenza di un Incaricato, laddove fosse indispensabile utilizzarne la password, il Responsabile ne chiede al custode la consegna. In tal caso il custode informa tempestivamente l'Incaricato che provvederà a sostituire la password.

Al custode compete altresì verificare che gli Incaricati utilizzino con diligenza la parola chiave, modificandola ove necessario (ad esempio: sospetta violazione della segretezza).

LE PRINCIPALI REGOLE PER UN CORRETTO TRATTAMENTO DEI DATI

a) Notificazione al Garante.

La liceità del trattamento è anzitutto subordinata ad un adempimento gravante sul Titolare: la notificazione al Garante di alcuni trattamenti di dati personali particolarmente suscettibili di recare pregiudizio ai diritti dell'interessato; si tratta, in particolare, di dati sensibili (dati genetici, dati inerenti lo stato di salute e la vita sessuale, dati attinenti alla personalità dell'interessato).

La notificazione va effettuata prima dell'inizio del trattamento e prima della cessazione del medesimo.

L'Università nella persona del Rettore – Titolare – ha provveduto ad effettuare la notificazione prescritta.

b) Diritti dell'interessato.

Secondo quanto enunciato all'art. 1 del Codice, accanto ai tradizionali diritti della personalità (nome, immagine, riservatezza), ogni soggetto (persona fisica) è titolare del diritto alla protezione dei dati.

Il Codice prevede che chiunque voglia utilizzare dati personali di un soggetto deve informarlo preventivamente, indicando con chiarezza l'uso che prevede di fare e le relative modalità (attraverso la c.d. "informativa" per la quale si rinvia al paragrafo successivo). In alcuni casi la persona interessata deve dare il proprio *consenso* (sul punto si rinvia al paragrafo relativo).

La vigente normativa riconosce all'interessato alcuni imprescindibili diritti, che devono essere salvaguardati nel corso di qualsivoglia trattamento:

a. il diritto di ottenere la conferma dell'esistenza di dati che lo riguardano e la relativa comunicazione;
b. il diritto di conoscere l'origine dei dati, le finalità e le modalità del trattamento, la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, gli estremi identificativi del titolare, dei responsabili e dei soggetti che possono venire a conoscenza dei dati;
c. il diritto di ottenere l'aggiornamento, la rettificazione, l'integrazione dei dati nonché la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
d. il diritto di opporsi per motivi legittimi al trattamento dei dati che lo riguardano;
e. il diritto di opporsi al trattamento a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

I diritti sono esercitati senza formalità, con richiesta rivolta al Titolare o al Responsabile, alla quale è fornito senza ritardo idoneo riscontro.

c) Informativa.

DATI PERSONALI E DATI SENSIBILI

L'informativa è una comunicazione (scritta o orale) effettuata dal Titolare nei confronti dell'interessato, prima dell'inizio del trattamento. Essa contiene le seguenti indicazioni:

- finalità e modalità del trattamento;
- natura obbligatoria o facoltativa del conferimento dei dati;
- conseguenze di un eventuale rifiuto di rispondere;
- i soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei medesimi;
- i diritti dell'interessato;
- gli estremi identificativi del Titolare e del Responsabile.

Esempi di informativa in uso presso l'Università sono: *l'informativa agli studenti* (resa all'atto dell'iscrizione o contestualmente alla richiesta di specifici servizi, come l'accesso alle Biblioteche o la fruizione dei servizi forniti dal Cosp); *l'informativa al personale* (relativa al trattamento da parte dell'Amministrazione, ai fini della gestione del rapporto di lavoro, dei dati dei propri dipendenti); *l'informativa ai fornitori* (allegata ai contratti o ai buoni d'ordine).

L'informativa è da fornire preferibilmente per iscritto all'interessato. Sono altresì possibili modalità diverse, come l'affissione di cartelli nei locali in cui gli interessati si recano per conferire i dati (segreterie Studenti, Uffici della Divisione del Personale …) o gli annunci on line (per quanto riguarda il trattamento dei dati connessi all'accesso al sito Internet d'Ateneo).

DATI PERSONALI IN AMBITO SANITARIO

L'informativa deve riguardare tutti i dati personali e deve essere fornita secondo le modalità sopra indicate, cui si aggiungono le seguenti specifiche condizioni:

- può riguardare il trattamento complessivo di tutti i dati trattati nell'interesse del paziente;
- può riguardare anche i dati raccolti presso terzi;
- è fornita per iscritto;
- deve indicare eventuali trattamenti che presentano rischi per i diritti e le libertà fondamentali (in particolare i trattamenti per scopi scientifici);
- riguarda anche il trattamento effettuato da altri soggetti (individuabili) ma correlato a quello effettuato dal medico o dall'organismo sanitario (es. prestazione specialistica). Ciò significa che l'informativa deve essere rilasciata da colui o coloro cui l'interessato ha chiesto la prima prestazione.

VIDEOSORVEGLIANZA

In caso di installazione di sistemi di videosorveglianza, l'informativa deve essere resa con modalità specifiche, attraverso pannelli che devono essere affissi in prossimità degli

ingressi alle strutture dove sono in funzione gli strumenti elettronici di rilevamento immagini, e che devono essere visibili da chi accede a tali strutture.

A tal proposito si rinvia al Provvedimento Generale dell'08/04/2010 in materia di *"Videosorveglianza"* nonché alla Circolare prot. 16668 del 16/05/2011.

d) Consenso.

Il Codice prevede che i soggetti pubblici, tra i quali l'Università, non devono richiedere il consenso dell'interessato.

Il consenso deve essere acquisito unicamente dagli esercenti le professioni sanitarie e dagli organismi sanitari pubblici (in ambito universitario tali sono le strutture le cui finalità sono: assistenza sanitaria, attività certificatorie, …), per i trattamenti riguardanti dati e operazioni indispensabili per perseguire finalità di tutela della salute e dell'incolumità fisica dell'interessato.

e) Sicurezza.

Il Codice riserva una particolare attenzione al profilo della sicurezza dei dati. Questi ultimi, infatti, risultano potenzialmente esposti ad alcuni *rischi*, quali, in particolare:

- distruzione o perdita (anche accidentale)
- accesso non autorizzato
- trattamento non consentito
- trattamento non conforme alle finalità della raccolta.

I soggetti che effettuano il trattamento devono operare in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi in questione.

Le misure di sicurezza sono distinte dal Codice in *"misure minime"*, espressamente richieste dalla legge per tutti i tipi di trattamento e volte ad assicurare un livello minimo di protezione, e ulteriori misure, individuate dall'iniziativa del Titolare, idonee a realizzare un livello più elevato di sicurezza, adeguato al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento.

Tra le misure di sicurezza è prevista la possibilità di redigere un *Documento sulla Sicurezza*, ossia un testo che comprenda:

- la descrizione dei trattamenti effettuati
- l'individuazione dei soggetti coinvolti nel trattamento
- l'analisi dei rischi che incombono sui dati
- la descrizione delle misure da adottare
- la previsione di interventi formativi a favore degli Incaricati del trattamento.

f) Responsabilità e sanzioni.

A chiusura della vigente disciplina il Testo Unico configura alcune ipotesi di *violazioni amministrative* (omessa o inidonea informativa all'interessato, omessa o incompleta notificazione al Garante, cessione dei dati al di fuori dei casi consentiti) e di *illeciti penali* (falsità nelle dichiarazioni e notificazioni al Garante, omissione di misure di sicurezza, inosservanza dei provvedimenti del Garante, altre ipotesi di violazione delle norme sul trattamento al fine di trarre profitto per sé o per altri o di arrecare danni a terzi).

Le prime sono punite con sanzioni consistenti nel pagamento di somme di denaro (fino a un massimo di € 60.000), i secondi con la reclusione fino a tre anni (o, in taluni casi, con l'ammenda sino a € 50.000).