Allegato 2)

COMPENDIO DELLA NORMATIVA SULLA PRIVACY PER IL TRATTAMENTO DEI DATI PERSONALI DELL'UNIVERSITÀ DEGLI STUDI DI PERUGIA

PREMESSA

La presente trattazione, che si colloca nell'ambito delle attività poste in essere dall'Università per favorire al proprio interno la diffusione e la corretta applicazione della normativa vigente in materia di privacy, riassume i principi e le nozioni più importanti della suddetta normativa, come modificata dal Codice emanato in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n. 196).

Per una più agevole consultazione, si è ritenuto utile articolare l'esposizione degli argomenti nei seguenti macro capitoli:

1. Il quadro normativo

2. Il significato di alcuni termini introdotti dalla normativa vigente

3. Le figure del Titolare, del Responsabile, dell'Incaricato, dell'Amministratore di sistema, del Preposto alla custodia delle parole chiave

4. La conoscenza dei principi e delle disposizioni normative in materia di privacy quale presupposto per la loro corretta applicazione nell'Ateneo

1. IL QUADRO NORMATIVO

Dal 1° gennaio 2004, con l'entrata in vigore del Codice in materia di protezione dei dati personali (cosiddetto Codice della privacy), tutti i precedenti provvedimenti normativi e regolamentari in materia di privacy (legge 675/96, D.Lgs 171/98, DPR 318/99, ecc.) sono da considerarsi abrogati.

Il Codice, infatti, oltre a razionalizzare, semplificare e coordinare in un "Testo Unico" tutte le precedenti disposizioni relative alla protezione dei dati personali, introduce importanti innovazioni, che tengono conto della "giurisprudenza" del Garante e della direttiva Ue 2002/58 sulla riservatezza nelle comunicazioni elettroniche.

Strutturalmente il Codice è diviso in tre parti (complessivamente 186 articoli). La prima è dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato. La seconda è la parte speciale dedicata a specifici settori, quali ad esempio l'ambito sanitario, il lavoro e la previdenza sociale, le comunicazioni elettroniche. La terza parte affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante. Sono inoltre allegati al Codice:

- **i codici di deontologia e di buona condotta (Allegato A)** relativi **(i)** all'attività giornalistica, **(ii)** agli scopi storici, **(iii)** agli scopi statistici e di ricerca scientifica nell'ambito del sistema statistico nazionale;
- **il disciplinare tecnico in materia di misure minime di sicurezza** (**allegato B**);
- **i trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia** (**allegato C**).

Saranno altresì allegati, via via che verranno adottati, anche gli altri codici di deontologia e di buona condotta attualmente in corso di predisposizione (Si segnala, in proposito, che con provvedimento del 13 maggio 2004 il Garante ha pubblicato in via provvisoria il testo relativo al Codice di deontologia e buona condotta, applicabile ai trattamenti di dati personali per scopi statistici e scientifici effettuati da Università, altri enti o istituti di ricerca e società scientifiche al di fuori del sistema statistico).
Il Codice ha la finalità di garantire che il trattamento dei dati personali 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. Tali garanzie sono estese anche ai diritti delle persone giuridiche (società private e pubbliche) e di ogni altro ente o associazione.

Il testo integrale del Codice privacy è consultabile sul sito **www.unipg.it**

2. IL SIGNIFICATO DI ALCUNI TERMINI INTRODOTTI DALLA NORMATIVA VIGENTE

2.1 Dati personali

Sono i dati relativi alle persone fisiche e giuridiche quali ad esempio il nome, il cognome, la data di nascita, la denominazione sociale, il codice fiscale, la partita iva, le immagini/fotografie, le pubblicazioni, le relazioni o report, le attestazioni, etc.. Sono altresì considerati dati personali quelli relativi al traffico telefonico in generale, alle e-mail ed ai c.d. *file di log*, cioè quelle informazioni attraverso le quali è possibile sapere quando, con chi e per quanto tempo ci si è collegati in rete (Internet, Intranet). Nella pratica, i suddetti dati sono anche definiti come "***dati comuni***" per distinguerli da quelli "***sensibili***" e "***giudiziari***".

I ***dati sensibili*** sono quelli che il Codice privacy definisce come dati personali idonei a rivelare, anche indirettamente:

- 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;
- lo stato di salute e la vita sessuale.

Nella tipologia dei dati sensibili sono da considerarsi ricompresi anche le semplici indicazioni utilizzate spesso nell'ambito della gestione del personale, come ad esempio: "iscritto al sindacato", "malato",

"aspettativa per malattia o maternità", fruizione di "permessi per visite mediche o per attività sindacali/politiche", "inidoneità" (psico-fisica, attitudinale, etc.).

I ***Dati giudiziari*** sono le informazioni rinvenibili nei provvedimenti emanati dal giudice penale per i quali è prevista la registrazione nel casellario giudiziale (art. 3 del DPR 313/02 in materia di casellario giudiziale), nonché i dati idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale. Si citano a titolo esemplificativo: le sentenze di condanna, i provvedimenti penali divenuti irrevocabili, i provvedimenti definitivi che riguardano misure di sorveglianza.

2.2 Rilevanti finalità d'interesse pubblico

Finalità, individuate dal D.lgs 196/2003 (vedi a mero titolo esemplificativo gli artt. 95 e 112) dalla legge o dal garante, connesse alle attività istituzionali dell'Università, che la stessa svolge per realizzare interessi pubblici in relazioni a funzioni ad essa attribuite, delegate o conferite dalla normativa statale e regionale vigente, nonché quelle inerenti l'organizzazione dell'Amministrazione Universitaria e lo sviluppo dell'attività amministrativa, nei suoi vari profili.

2.3 Trattamento

In sintesi significa **"utilizzo"** dei dati personali. Più precisamente, il Codice della privacy lo definisce come *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 di dati.*

2.4 Banche di dati

Sono gli archivi (cartacei o elettronici/informatici) che contengono i dati oggetto di trattamento.

2.5 Interessato

E' la persona fisica, persona giuridica, ente o associazione cui si riferiscono i dati personali.

2.6 Garante per la protezione dei dati personali (o semplicemente Garante)

Autorità posta a garanzia del rispetto delle norme sulla privacy. E' un organo collegiale costituito da quattro membri (commissari) e da un Segretario Generale. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione. Riceve, tra l'altro, le segnalazioni ed i ricorsi da parte degli interessati in relazione a presunte violazioni della normativa (dinieghi di "accesso" e/o trattamenti illeciti), emettendo al riguardo eventuali provvedimenti nei confronti del Titolare/Responsabile.

2.7 Misure minime di sicurezza

Sono il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste dal Codice della privacy, che configurano il livello minimo di protezione dei dati personali.

2.8 Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

2.9 Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

2.10 Credenziali di autenticazione

I dati ed i dispositivi, in possesso di una persona, da questi conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica. Servono sia a proteggere i dati che a riconoscere l'incaricato, e di conseguenza il suo profilo e i suoi permessi. Possono accedere agli strumenti elettronici solo gli incaricati dotati di credenziali di autenticazione che consentano il positivo superamento della procedura di autenticazione prevista per quel trattamento. Le credenziali di autenticazione sono costituite da un codice identificativo dell'incaricato, la cosiddetta componente pubblica delle credenziali, e da una parola chiave riservata; in altre parole i classici: user ID e password.

2.11 User ID

E' un codice identificativo personale formato da lettere e/o numeri. Viene sempre abbinato alla password (segreta).

2.12 Password

E' la parola chiave, componente di una credenziale di autenticazione associata ad una persona e a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica, che serve per accordare l'accesso al sistema informatico agli utenti.

2.13 Profilo di autorizzazione

E' l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti. Quando sono previsti diversi livelli di accesso ai dati, deve essere previsto un sistema di autorizzazione che riconosca i vari profili ed i relativi permessi. I profili possono essere personalizzati o previsti per specifiche categorie di utenti. Tali profili vanno configurati anteriormente all'inizio del trattamento. In questo modo, infatti, l'accesso viene limitato ai soli dati necessari per effettuare le operazioni di trattamento in relazione ai permessi di quel profilo.

2.14 Sistema di autorizzazione

E' l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

LE FIGURE DEL TITOLARE, DEL RESPONSABILE, DELL'INCARICATO, DELL'AMMINISTRATORE DI SISTEMA E DEL PREPOSTO ALLA CUSTODIA DELLE PAROLE CHIAVE

3.1 IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Il Titolare del trattamento è il soggetto (persona fisica, società, enti pubblici o qualsiasi altro ente, associazione od organismo) che, nel raccogliere i dati personali (direttamente dall'interessato od anche attraverso la cessione da parte di altri) decide come ed in base a quali finalità (ad esempio per rapporto di lavoro, per finalità didattica, etc.) effettuerà il trattamento dei dati raccolti. Pertanto, ai sensi di legge, l'Università degli Studi di Perugia è "Titolare" dei dati personali da essa trattati con l'ausilio dei mezzi informatici o cartacei ecc.;

3.2 IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Il Codice della privacy prevede la facoltà, per il Titolare, di nominare uno o più Responsabili del trattamento; è altresì previsto che possa essere nominato "Responsabile" non solo una persona fisica ma anche una società o altri organismi come gli enti, le associazioni, ecc.. Inoltre, la designazione può riguardare più soggetti (per esempio in presenza di una struttura molto articolata).
Il Titolare individua il Responsabile tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza. Di conseguenza, in relazione alla sua articolata struttura, l'Università degli Studi di Perugia, nella persona del Rettore, ha ritenuto opportuno nominare, con Decreto Rettorale n.1077 dell'1 giugno 2004, "**Responsabili**" del trattamento dei dati:

A) Per ciò che attiene le Strutture amministrative afferenti alla Sede Centrale:

- Il **Direttore Amministrativo**, relativamente ai dati trattati dall'Ufficio Organi Collegiali, dall'Ufficio Archivio e Protocollo, dalla Segreteria della Direzione Amministrativa e dal "Laboratorio per la formazione, lo sviluppo e l'organizzazione delle persone";
- I **Dirigenti**, ciascuno relativamente ai dati trattati dalle rispettive Ripartizioni;

B) Per ciò che attiene il Servizio per la Gestione e lo sviluppo della rete di Ateneo:

- Il **Presidente del Comitato Tecnico Scientifico del Servizio di Rete**, relativamente ai dati trattati nell'ambito del predetto Servizio;

C) Per ciò che attiene le Strutture di coordinamento, didattiche, di ricerca, e di servizio:

- I **Presidi**;
- I **Presidenti dei Corsi di laurea**;

- I **Direttori di Dipartimento**;
- I **Direttori dei Centri di Ricerca**;
- I **Direttori dei Centri di Servizio**;
- I **Direttori di Scuole di Specializzazione**;

Ciascuno relativamente ai dati trattati dalle rispettive Strutture;

D) Per ciò che attiene l'Azienda Agraria:

- Il **Consigliere Amministratore Delegato**, relativamente ai dati trattati nell'ambito dell'Azienda medesima;

E) Per ciò che attiene il Polo Didattico e Scientifico di Terni:

- Il **Pro Rettore delegato del Rettore**, relativamente ai dati trattati nella relativa Struttura;

F) Per ciò che attiene i dati trattati dalla Segreteria del Rettorato, dalla Struttura in Staff denominata "Progetto Comunicazione e Relazioni Esterne" e dal Nucleo di Progettazione Universitaria, il **Rettore** ne mantiene la responsabilità diretta;

Inoltre l'Ateneo si è riservato di effettuare, comunque, ulteriori nomine di "Responsabili" laddove si rendesse necessario, per lo svolgimento di attività istituzionali, comunicare e/o delegare a soggetti terzi esterni all'Ateneo il trattamento di alcuni dati.

3.3 L'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

L'Incaricato è la persona fisica alla quale, nell'ambito delle proprie attività, il Titolare o il Responsabile affidano il trattamento dei dati personali (elaborazione, archiviazione, ecc.). L'Incaricato è, dunque, colui che operativamente effettua i "trattamenti", attenendosi alle istruzioni del Titolare o del Responsabile.

L'Università degli Studi di Perugia affida ai Responsabili il compito di nominare "Incaricati" le persone fisiche, in relazione alle attività (e quindi ai trattamenti di competenza), svolte nell'ambito della struttura universitaria di appartenenza, impartendo loro adeguate istruzioni.

3.4 L'AMMINISTRATORE DI SISTEMA

L'Amministratore di sistema è il soggetto che si occupa del sistema informatico e delle risorse operative. Come previsto dal D.R. n. 1077 dell'1 giugno 2004, la nomina dei suddetto Amministratore di Sistema, per l'Amministrazione Centrale è affidata al Dirigente della Ripartizione Servizi Informatici e Statistici, mentre per le Strutture esterne ai Singoli Responsabili delle stesse, ove necessario.

Compete all'Amministratore di Sistema:

a Attribuire a ciascun incaricato del trattamento, un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice non potrà neppure in tempi diversi, essere assegnato a persone diverse;

b Assegnare e gestire i codici identificativi personali prevedendone la disattivazione nel caso di perdita della qualità che ne consente l'accesso all'elaboratore, ovvero nel caso di loro mancato utilizzo per un periodo superiore a sei mesi;

c Disporre ogni opportuna misura e ogni adeguata verifica, per evitare che soggetti non autorizzati possano avere accesso agli archivi delle parole chiave se leggibili;

d Provvedere affinché gli elaboratori del sistema informativo siano protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615 *quinquies* cod.pen., mediante idonei programmi la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale;

e Assistere il Responsabile del trattamento in particolare per quanto concerne l'analisi dei rischi presso la propria Struttura e per le informazione che il Responsabile è tenuto ad inviare al Titolare per la stesura annuale del Documento Programmatico di Sicurezza (DPS).

3.5 PREPOSTI ALLA CUSTODIA DELLE PAROLE CHIAVE

Il punto 10 dell'all. B. "Disciplinare tecnico" del Codice Privacy individua un "Preposto alla custodia delle parole chiave" il quale deve garantirne la segretezza e qualora , in assenza dell'incaricato, venga effettuato un trattamento utilizzando le stesse, deve tempestivamente informarne l'incaricato medesimo.

Compete al Preposto:

a Custodire, per un eventuale accesso di emergenza, la busta chiusa, controfirmata contenente il modulo utilizzato dal singolo incaricato per indicare la parola chiave dallo stesso prescelta;

b Accertare costantemente che gli incaricati utilizzino la parola chiave con diligenza e che la modifichino ogni qualvolta sussista il dubbio che essa sia stata manomessa. In tale occasione occorrerà provvedere all'aggiornamento della parola chiave contenuta in busta chiusa.

LA CONOSCENZA DEI PRINCIPI E DELLE DISPOSIZIONI NORMATIVE IN MATERIA DI PRIVACY QUALE PRESUPPOSTO PER LA LORO CORRETTA APPLICAZIONE

Occorre introdurre, in via preliminare, alcuni principi generali sui quali si basano le procedure e le modalità operative poste in essere dall'Università per una corretta applicazione della normativa vigente in materia di privacy.

In particolare:

a) i dati personali devono essere trattati:

- in osservanza dei criteri di riservatezza (ad esempio, non devono essere resi noti a persone non interessate/autorizzate) e rispettando le istruzioni dell'Ateneo sulla classificazione e gestione delle informazioni);
- in modo lecito e secondo correttezza (ad esempio, previa informativa e consenso dell'interessato);
- conservati in una forma che consenta l'identificazione dell'interessato (ad esempio aggiornandoli, anche in base alle indicazioni fornite dall'interessato stesso) e per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (non oltre il tempo

impiegato per fornire all'interessato una certa prestazione richiesta o per svolgere una determinata attività);

b) i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi, anche accidentali, di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

4.1 Informativa all'interessato

Per informativa si intende, in sintesi, la comunicazione agli interessati delle informazioni riguardanti le finalità (ad esempio gestione del rapporto di lavoro, iscrizione studenti ecc.) e le modalità di utilizzo (in modo automatico, tramite supporto elettronico, attraverso l'elaborazione di terzi, ecc.) dei dati personali raccolti e successivamente trattati. Nell'informativa è prevista, inoltre, l'indicazione dei diritti che l'interessato può esercitare in relazione al trattamento dei suoi dati (accesso, modifica, cancellazione, ecc.) ed il nominativo/denominazione sociale ed indirizzo del Titolare; è prevista, altresì, l'indicazione dei soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati del trattamento. L'informativa può essere fornita all'interessato sia per iscritto che verbalmente.

Consenso dell'interessato

I soggetti pubblici, ai sensi dell'art. 18, comma 4, non devono richiedere il consenso dell'interessato salvo quanto previsto nella parte II del Codice Privacy per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici. Il trattamento di dati diversi da quelli sensibili e giudiziari è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente, fermo restando che sia necessario per lo svolgimento delle funzioni istituzionali.

4.2 Diritti dell'interessato

Nel linguaggio comune, con una formula molto approssimativa ma efficace, si è ormai abituati ad identificare i diritti dell'interessato con il c.d. *diritto di accesso*, diritto, si badi bene, che il legislatore ha riconosciuto solo all'interessato e non a chiunque, dando però all'interessato stesso la possibilità di delegare per iscritto altre persone fisiche o associazioni. In sintesi, l'interessato ha il diritto di ottenere a cura del Titolare o del Responsabile, senza ritardo:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;
- la comunicazione dei medesimi dati e della loro origine;
- la cancellazione, la trasformazione in forma anonima (cioè in forma aggregata o con la cancellazione dei riferimenti che, direttamente o indirettamente, possano far risalire all'interessato) o il blocco dei

dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

- l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;
- di conoscere i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati del trattamento.

Inoltre, l'interessato ha il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano.

4.3 Cessazione del trattamento

Ci si riferisce alla cessazione del trattamento quando per qualsiasi motivo i dati vengono distrutti (volontariamente od anche accidentalmente), ovvero ceduti a terzi cessandone il relativo trattamento.

4.4 Sicurezza dei dati personali

"Per essere efficace, la protezione dei dati deve comprendere anche una disciplina rigorosa della sicurezza". Basandosi su questo principio il legislatore ha introdotto una prima norma generale sulla sicurezza dei dati nell'ambito dell'articolo 31 del Codice della privacy, dettagliando poi i singoli adempimenti nei successivi articoli 32-36 e nell'allegato B del Codice.

In particolare, il suddetto allegato B, intitolato "Disciplinare tecnico in materia di misure minime di sicurezza", disciplina in maniera puntuale e rigorosa le misure minime da adottare per garantire la sicurezza fisica, logica e organizzativa dei dati personali. L'intera disciplina è ispirata al principio generale sancito dal citato articolo 31, secondo il quale: *"i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"*.

Le modalità operative e le informazioni di carattere tecnico in materia di misure minime di sicurezza sono disponibili nelle istruzioni agli Incaricati del trattamento dei dati personali comuni, sensibili e/o giudiziari.

4.5 Sanzioni

Le sanzioni previste dalla normativa vigente (di cui agli articoli da 161 a 172 del Codice privacy) a fronte di eventuali inadempimenti o di trattamenti illeciti di dati personali possono essere, a seconda del tipo di inosservanza, di natura amministrativa (fino ad un massimo di 60.000 Euro) o penale (fino a 3 anni di reclusione).