UNIVERSITÀ
degli STUDI di LECCE
DIREZIONE AMMINISTRATIVA
Viale Gallipoli, 49 – 73100 Lecce
☎ +39 0832292210 Fax +39 0832292212

Prot. n. 15546

Lecce, 24 giugno 2004

Ai Presidi di Facoltà
Ai Direttori di Dipartimento e dei Centri con autonomia contabile e gestionale
Ai Responsabili di Progetto
Ai Direttori delle Scuole di Specializzazione
Al Direttore del Centro Linguistico di Ateneo
Al Direttore Amministrativo
Al Capo di Gabinetto del Rettore
Ai Direttori di Area
Al Direttore del Centro Servizi Grandi Progetti
Al Coordinatore Generale Servizi Bibliotecari
Al Coordinatore Generale del SIBA
Al Direttore della Biblioteca Interfacoltà
Al Coordinatore del G.I.S.I.

LORO SEDI

OGGETTO: Misure minime di sicurezza previste dal D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali)

Come già anticipato nella precedente nota n. 11035 del 12 maggio u.s., si forniscono alle SS.LL., Responsabili del trattamento dei dati personali, ulteriori opportune indicazioni in ordine alla concreta predisposizione delle misure di sicurezza previste dal Decreto Legislativo citato in oggetto (consultabile nella versione aggiornata all'indirizzo web www.garanteprivacy.it, link normativa italiana).

Le misure minime di sicurezza, ossia le misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione dei dati personali, sono, più in generale, elencate agli art. 33, 34 (Trattamenti con strumenti elettronici) e 35 (Trattamento senza l'ausilio di strumenti elettronici) del Codice in materia di protezione dei dati personali (di seguito denominato Codice), mentre i dettagli realizzativi sono illustrati nell'Allegato B) dello stesso Codice (Disciplinare tecnico in materia di misure minime di sicurezza, di seguito denominato Disciplinare tecnico). Tale distinzione consente una revisione periodica del dettaglio delle misure minime mediante l'aggiornamento del solo disciplinare (con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e la tecnologia) senza modificare il Codice.

L'articolo 34 (trattamenti con strumenti elettronici) prevede le seguenti misure minime di sicurezza (nei modi previsti dal disciplinare tecnico):

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli

UNIVERSITÀ
degli STUDI di LECCE
DIREZIONE AMMINISTRATIVA
Viale Gallipoli, 49 – 73100 Lecce
☎ +39 0832292210 Fax +39 0832292212

incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- 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.

L'articolo 35 (trattamenti senza l'ausilio di strumenti elettronici) prevede le seguenti misure minime di sicurezza (nei modi previsti dal disciplinare tecnico):
a) aggiornamento periodico 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.

Si distinguono quindi, con il nuovo Codice, i "trattamenti con strumenti elettronici" dai "trattamenti senza l'ausilio di strumenti elettronici", e viene eliminata la previsione del D.P.R. 318/1999 relativa all'"elaboratore connesso ad altri elaboratori attraverso reti di telecomunicazioni disponibili al pubblico".

TRATTAMENTO CON STRUMENTI ELETTRONICI

Con riferimento ai trattamenti con strumenti elettronici, dovranno essere adottate le modalità tecniche di seguito specificate.

Sistema di autenticazione informatica

Deve essere utilizzato un sistema di autenticazione informatica che consenta di verificare e convalidare in modo certo e univoco l'identità di chiunque acceda agli elaboratori e a tutti gli strumenti software utilizzati per il trattamento dei dati. I meccanismi di autenticazione comprendono tutti quelli normalmente utilizzati, quali le password, la smart card, il certificato digitale, ecc. Deve essere prevista una specifica politica di generazione, utilizzo, custodia, aggiornamento e distruzione dei meccanismi di autenticazione, (punti 1-11 del Disciplinare tecnico). Ad esempio:

- bisogna impartire precise istruzioni agli incaricati affinché adottino le necessarie cautele per assicurare la segretezza delle loro credenziali e conservino diligentemente gli eventuali dispositivi necessari per l'autenticazione (punto 4);
- la password deve essere lunga almeno 8 caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato a cui appartiene (punto 5);

UNIVERSITÀ
degli STUDI di LECCE
DIREZIONE AMMINISTRATIVA
Viale Gallipoli, 49 – 73100 Lecce
☎ +39 0832292210 Fax +39 0832292212

- la password deve essere modificata dall'incaricato al primo utilizzo e successivamente almeno ogni sei mesi. Nel caso di trattamento di dati sensibili e di dati giudiziari la password deve essere cambiata ogni tre mesi (punto 5);
- devono essere disattivate le credenziali di autenticazione non utilizzate da almeno sei mesi (punto 7);
- devono essere impartite precise disposizioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati (punto 9);
- devono essere previste specifiche azioni per assicurare la disponibilità di un particolare trattamento dei dati, anche nel caso di un prolungata assenza o impedimento (per esempio, a causa di una malattia) degli incaricati normalmente preposti al suddetto trattamento (punto 10).

Sistema di autorizzazione

- Nel caso di utilizzo di incaricati con compiti distinti per il trattamento dei dati, come nel caso in cui alcuni possono solo visualizzare i dati ed altri possono anche modificarli, deve essere adottato e gestito un sistema di accesso ai dati ed ai sistemi basato sui cosiddetti "profili di autorizzazione" (punto 12). I profili definiscono in dettaglio le azioni consentite a ogni classe di incaricati e indicano le impostazioni da assegnare agli strumenti elettronici che realizzano i meccanismi di autorizzazione (punto 13), realizzando il need-to-know, ovvero una efficace politica di autorizzazione per l'accesso ai dati;
- la verifica circa la validità delle definizioni dei profili di autorizzazione deve essere effettuata periodicamente e, comunque, almeno una volta all'anno (punto 14).

Protezione di dati e sistemi

I dati ed i sistemi elettronici devono essere protetti da accessi non consentiti che possono comprometterne la loro sicurezza. Le misure minime da predisporre devono prevedere:

a) l'uso di procedure e di software che contrastino i virus informatici e le altre tipologie di malfare, quali, ad esempio, i worm, i cavalli di Troia, gli stealth, ecc. L'aggiornamento di tali software deve avvenire con cadenza almeno semestrale (punto 16);
b) l'applicazione periodica e regolamentata da apposite procedure degli aggiornamenti dei sistemi operativi e dei software utilizzati (patch, service pack e hotfix), al fine di eliminare le nuove vulnerabilità e gli errori nel software (bug) (punto 17);
c) l'adozione di misure procedurali e tecniche che prevedano il salvataggio dei dati con cadenza almeno settimanale, al fine di salvaguardare l'integrità e la disponibilità dei dati (punto 18);
d) l'adozione di uno specifico programma di formazione rivolto agli incaricati, al fine di minimizzare il rischio di un utilizzo improprio degli strumenti elettronici.

Le misure appena descritte dovranno essere ulteriormente rafforzate nel caso in cui si effettui il trattamento di **dati sensibili o giudiziari**.

UNIVERSITÀ
degli STUDI di LECCE
DIREZIONE AMMINISTRATIVA
Viale Gallipoli, 49 – 73100 Lecce
☎ +39 0832292210 Fax +39 0832292212

Per dati sensibili si intendono (articolo 4, comma 1, punto d) i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Per dati giudiziari (articolo 4, comma 1, punto e) si intendono alcune informazioni riguardanti il rapporto tra il cittadino e la giustizia penale, come, ad esempio, le condanne penali passate in giudicato, la sospensione condizionale e la non menzione della pena, le misure di sicurezza personali e patrimoniali.

Per i dati sensibili e giudiziari si applicano le misure minime previste ai punti 20-24 del disciplinare tecnico.

Protezione di dati e sistemi

Devono essere rafforzate le misure minime mediante protezione contro gli accessi abusivi (punto 20). Di regola i due principali strumenti di sicurezza da adottare sono i firewall e i sitemi di rilevamento delle intrusioni (Ids: Intrusion detection systems). I firewall, utilizzati ormai comunemente per proteggere tutte le reti aziendali che hanno una connessione ad internet, sono strumenti attivi che cercano di bloccare i tentativi di intrusione nel momento stesso in cui si realizzano. Gli Ids, invece, sono strumenti di sicurezza ancora poco diffusi, in quanto la loro corretta realizzazione e gestione è particolarmente onerosa dal punto di vista economico ed organizzativo. Il loro utilizzo ha la finalità principale di rivelare e registrare delle attività non consuete su una rete aziendale, che potrebbero essere successivamente riconosciute come parti costitutive di un attacco alla sicurezza dei dati. Le informazioni raccolte dagli Ids vengono analizzate periodicamente off-line da personale qualificato, al fine di individuare eventuali tentativi di attacco o vulnerabilità residue ancora presenti nel sistema informativo. Quindi il ruolo degli Ids è di regola di tipo passivo, in quanto non intervengono direttamente nel bloccare le intrusioni. Tuttavia essi sono di fondamentale importanza per migliorare le misure di sicurezza nel loro complesso. E' opportuno, pertanto, prevedere l'addestramento di una o più persone che sappiano gestire in modo efficace le fasi critiche per la sicurezza.

Copie di sicurezza e disponibilità dei dati

Devono essere apportate idonee misure di sicurezza per garantire, nel caso di danneggiamento fortuito o intenzionale dei dati o degli strumenti elettronici, il ripristino della disponibilità dei dati stessi. Tale misura dovrà essere resa possibile in un periodo non superiore a sette giorni, al fine di tutelare i diritti degli interessati al trattamento (punto 23). Tutto ciò impone l'effettuazione di copie di riserva dei dati e la verifica che tali copie siano effettivamente utilizzabili per un eventuale ripristino del servizio. Le copie di riserva dovranno essere adeguatamente conservate e protette da accessi non autorizzati (punto 21), prevedendo sia opportune misure procedurali, organizzative e logistiche (come ad esempio la conservazione in locali particolarmente protetti), sia adottando specifiche misure tecniche (come ad esempio la cifratura dei dati). In casi più complessi potrebbe essere indispensabile la predisposizione di una strategia di tipo Disaster Recovery, che definisca,

UNIVERSITÀ
degli STUDI di LECCE
DIREZIONE AMMINISTRATIVA
Viale Gallipoli, 49 – 73100 Lecce
☎ +39 0832292210 Fax +39 0832292212

nell'ipotesi di eventi catastrofici (terremoti, inondazioni) le procedure tecniche ed organizzative alternative e sostitutive a quelle normalmente utilizzate. Dovrà essere infine assicurato che il riutilizzo dei supporti che contenevano i dati sensibili o giudiziari è permesso solo se le informazioni precedentemente immagazzinate non siano in alcun modo ripristinabili (punto 22).

Cifratura e separazione dei dati

Il Disciplinare tecnico (punto 19.8 e punto 24) stabilisce che i dati personali idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari o da esercenti le professioni sanitarie devono essere protetti o attraverso l'utilizzo di tecniche di cifratura, o operando una separazione tra tali dati e gli altri dati personali che consentono di identificare direttamente gli interessati. In particolare, i dati relativi all'identità genetica devono essere trattati esclusivamente all'interno di locali particolarmente custoditi ed accessibili ai soli incaricati dei trattamenti o ad altri soggetti espressamente autorizzati (punto 24). Bisognerà altresì predisporre ulteriori misure di sicurezza nel caso fosse necessario il trasferimento su supporti elettronici dei suddetti dati dai locali normalmente dedicati al loro trattamento: in tale ipotesi dovrà essere predisposta la cifratura dei dati e il trasporto dovrà avvenire in contenitori muniti di serratura o dispositivi equivalenti (punto 24).

TRATTAMENTO SENZA STRUMENTI ELETTRONICI

Qualora si effettui il trattamento di dati personali senza l'ausilio di strumenti elettronici dovranno essere adottati un insieme minimo di misure di sicurezza, di tipo procedurale, organizzativo e logistico. In particolare:

- devono essere impartite istruzioni scritte finalizzate al controllo ed alla custodia degli atti e dei documenti contenenti dati personali durante l'intero ciclo necessario allo svolgimento delle operazioni di trattamento dei dati (punto 27);
- devono essere aggiornati con cadenza almeno annuale i profili di autorizzazione e l'ambito del trattamento consentito ai singoli incaricati o a classi di incaricati (punto 27). Anche in questo caso, così come nella ipotesi di trattamento con strumenti elettronici, occorrerà realizzare una politica di accesso ai dati del tipo need-to-know;
- deve essere previsto l'obbligo, da parte degli incaricati, di custodire e controllare gli atti e i documenti a loro affidati e contenenti dati personali sensibili e giudiziari. In tal modo viene impedito l'accesso anche momentaneo a tali documenti da parte di persone non autorizzate (punto 28);
- dovrà essere controllato e regolamentato l'accesso, anche dopo l'orario di chiusura, agli archivi contenenti dati sensibili o giudiziari (punto 29).

Le misure minime di sicurezza appena descritte dovevano essere adottate entro il 30 giugno 2004 (art. 180 D.lgs. 196/2003). Tuttavia, il 22 giugno u.s., il Consiglio dei Ministri ha varato un decreto legge, di prossima pubblicazione in Gazzetta Ufficiale, che, modificando l'art. 180 del Codice, proroga al 31 dicembre 2004 l'adozione delle misure di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) del Codice.

UNIVERSITÀ
degli STUDI di LECCE
DIREZIONE AMMINISTRATIVA
Viale Gallipoli, 49 – 73100 Lecce
☎ +39 0832292210 Fax +39 0832292212

Si fa presente che la nuova scadenza (come anche quella originaria del 30 giugno) riguarda solo le misure minime di sicurezza "nuove" previste dal Codice, non già quelle esplicitamente previste dalla precedente normativa (ed in particolare dal DPR 318/1999), per le quali il termine per l'adozione era stato fissato per il 31 dicembre 2000.

Sanzioni

Il Codice distingue le violazioni amministrative (art. 161-166) e gli illeciti penali (art. 167-172). E' considerato illecito penale, ed in particolare reato contravvenzionale, la violazione dell'obbligo di adozione delle misure minime di protezione dei dati personali (art. 169, comma 1): *chiunque, essendovi tenuto, omette di adottare tali misure è punito con l'arresto sino a due anni o con l'ammenda da 10.000 euro fino a 50.000 euro.*

MISURE DI SICUREZZA "IDONEE"

E' opportuno ricordare che l'adozione delle misure di sicurezza, se consente di evitare l'applicazione della sanzione penale prevista dall'art. 169, comma 1, del Codice, appena enunciato, non è sufficiente per liberare i soggetti che effettuano il trattamento dei dati da eventuali profili di responsabilità in sede civile. L'art. 15 del Codice, infatti, dispone che "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile" (Responsabilità per l'esercizio di attività pericolose). I soggetti che trattano i dati dovranno dimostrare di aver adottato tutte le misure idonee (non solo quelle minime) ad evitare il danno. Le misure "idonee" sono disciplinate all'art. 31 del Codice: "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". E' evidente che non è possibile, come invece nel caso delle misure minime, predisporre un elenco delle misure da adottare al fine di evitare la responsabilità civile. Bisognerà attendere l'intervento della giurisprudenza per avere dei criteri orientativi, fra i quali vi potrebbe rientrare la proporzionalità fra natura dei dati da proteggere e costi delle misure da adottare. Attualmente, il riferimento è costituito da tutte le misure idonee, *allo stato dell'arte*, a evitare il danno.

Si ricorda infine che, ai sensi dell'art. 15, comma 2, del Codice, il danno non patrimoniale causato al soggetto del quale viene trattato il dato personale è risarcibile anche in caso di violazione dell'art. 11 (relativo alle modalità del trattamento ed ai requisiti dei dati, che devono essere trattati in modo lecito e secondo correttezza). In tale ipotesi il soggetto danneggiato ha diritto al risarcimento, nei casi previsti dalla legge, delle sofferenze fisiche o psichiche subite, e che costituisce appunto il danno non patrimoniale.

VIDEOSORVEGLIANZA E CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI PER SCOPI STATISTICI E SCIENTIFICI

Da ultimo, in allegato alla presente nota, si trasmettono:

UNIVERSITÀ
degli STUDI di LECCE
DIREZIONE AMMINISTRATIVA
Viale Gallipoli, 49 – 73100 Lecce
☎ +39 0832292210 Fax +39 0832292212

1) il provvedimento generale del 29 aprile u.s. del Garante per la protezione dei dati personali in materia di videosorveglianza;
2) il Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, sottoscritto il 13 maggio u.s. in via preliminare, tra gli altri, anche dalla Conferenza dei Rettori delle Università Italiane.

Si invitano le SS.LL. a diffondere i documenti appena enunciati nell'ambito delle strutture di rispettiva competenza, al fine di consentire la corretta applicazione delle disposizioni in essi contenute.

Si confida nella collaborazione delle SS.LL. per consentire una effettiva ed efficace attuazione della complessa normativa nell'ambito dell'Ateneo.

La documentazione citata nella presente nota è pubblicata anche sul sito dell'Ateneo http://www.unile.it/ateneo/ateneo/privacy.

Per ogni possibile chiarimento od informazione le SS.LL. possono fare riferimento all'Avv Antonio Bax, funzionario in servizio presso la Direzione Amministrativa (tel. 0832/292221, fax 0832/292212, e-mail antonio.bax@ateneo.unile.it).

IL RETTORE

(Prof. Oronzo Limone)