



Decreto prot. n. 6804/I/003

Oggetto: Decreto rettorale di modifica del Regolamento sulle Misure attuative del Codice per la protezione dei dati personali, ai sensi del decreto legislativo 30.6.2003, n.196. - Documento programmatico sulla sicurezza - DPS.

IL RETTORE

RICHIAMATO il decreto legislativo del 30.6.2003, n. 196 "Codice in materia di protezione dei dati personali" che garantisce 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;

RICHIAMATO il Regolamento sulle Misure attuative del Codice per la protezione dei dati personali, ai sensi del decreto legislativo 30.6.2003, n.196. - Documento programmatico sulla sicurezza - DPS modificato con decreto rettorale prot. n. 6704/I/003 del 29.3.2010;

CONSIDERATO che il decreto legislativo del 30.6.2003, n. 196 prevede l'aggiornamento annuale del Documento programmatico sulla sicurezza;

RICHIAMATI in particolare la deliberazione del Consiglio di Amministrazione del 6.7.2010, punto 6, di modifica alla struttura amministrativa dell'Università;

PRESO ATTO di dover conseguentemente aggiornare gli allegati al Regolamento sulle Misure attuative del Codice per la protezione dei dati personali, ai sensi del decreto legislativo 30.6.2003, n. 196. - Documento programmatico sulla sicurezza - DPS ed in particolare gli allegati A "Strutture preposte ai trattamenti" e B "Elenco dei trattamenti";

SENTITI i responsabili delle strutture preposte ai trattamenti dei dati, che hanno comunicato gli aggiornamenti da apportare agli allegati del Regolamento sulle Misure attuative del Codice per la protezione dei dati personali, in particolare agli allegati A e B, mentre l'allegato C rimane invariato;

D E C R E T A

Art. 1

Sono modificati gli allegati A e B del Regolamento sulle Misure attuative del Codice per la protezione dei dati personali, ai sensi del decreto legislativo 30.6.2003, n.196.

Art. 2

Il presente decreto è pubblicato sul sito informatico dell'Università nella sezione "Albo di Ateneo" ed entra in vigore con decorrenza immediata.

Art. 3

I Regolamento nella versione integrale modificata è pubblicato sul sito informatico dell'Università nella sezione "Atti e documenti > Regolamenti" .

Bergamo, 30.3.2011

IL RETTORE
F.to Prof. Stefano Paleari

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

MISURE ATTUATIVE DEL CODICE PER LA PROTEZIONE DEI DATI PERSONALI, ai sensi del decreto legislativo 30.06.2003 N. 196.

I^a PARTE

INDICE:

Articolo 1 - Ambito di applicazione	4
Articolo 2 - Definizioni	4
Articolo 3 - Titolare, responsabili e incaricati del trattamento dei dati	4
Articolo 4 – Monitoraggio dei dati personali e operazioni eseguibili	4
Articolo 5 - Diritti dell'interessato	4
Articolo 6 - Obblighi di informativa	4
Articolo 7 – Codice di deontologia e di buona condotta	4

Articolo 1 - Ambito di applicazione

Fermo restando la disciplina specifica emanata con d.lgs. 30.06.2003 n. 196 il presente Regolamento viene adottato al fine di garantire l'attuazione del "Codice" in materia di protezione dei dati personali, all'interno dell'Università degli Studi di Bergamo e la redazione del Documento programmatico sulla sicurezza (DPS).

Sono esclusi dalla disciplina del presente Regolamento i trattamenti di dati raccolti dal personale docente e ricercatore dell'Università per lo svolgimento della propria attività didattica.

Articolo 2 - Definizioni

Circa le definizioni contenute nel presente atto, si rinvia all'art. 4 del d.lgs. 196/2003.

Articolo 3 - Titolare, responsabili e incaricati del trattamento dei dati

L'Università degli Studi di Bergamo è titolare dei dati personali detenuti dall'Università stessa, raccolti o meno in banche di dati, automatizzate o cartacee.

Le responsabilità e i compiti declinati dall'art. 29 del Codice sono attribuite ai Responsabili di Servizio o di posizione organizzativa (Uffici di Staff e Presidi di Facoltà e Dipartimenti), ai Direttori di Dipartimento, ai Direttori dei Centri di ricerca e di servizio di Ateneo, ai Direttori dei Centri di ricerca e di servizio di Facoltà e di Dipartimento.

Questi affidano ai propri collaboratori l'incarico del trattamento dei dati tenendo conto dell'esperienza, del livello di preparazione e di responsabilizzazione nell'attività assegnata.

Articolo 4 – Monitoraggio dei dati personali e operazioni eseguibili

Successivamente all'applicazione del presente articolato, il titolare del trattamento provvederà, ad effettuare periodicamente l'aggiornamento ricognitivo dei dati trattati e delle operazioni eseguite.

Articolo 5 - Diritti dell'interessato

L'interessato gode dei diritti di accesso ai dati personali che trovano riscontro puntuale all'art. 7 del d.lgs. 196/2003.

Articolo 6 - Obblighi di informativa

Ai sensi dell'art. 13 del d.lgs. 196/2003, ogni singola struttura provvede ad informare oralmente o per iscritto l'interessato previamente alla raccolta dei dati personali circa:

- a) le finalità e le modalità del trattamento cui sono destinati i dati;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- e) i diritti riconosciuti all'interessato dagli artt. 7 e ss. del d.lgs. 196/2003;
- f) il nome, la denominazione o la ragione sociale ed il domicilio, la residenza o la sede del titolare e del responsabile del trattamento dei dati.

L'informativa può essere resa oralmente, per iscritto, nel modulo di iscrizione, in documenti disponibili presso le strutture o anche mediante avviso pubblico.

Articolo 7 – Codice di deontologia e di buona condotta

L'Università si impegna a sottoscrivere il codice di deontologia e di buona condotta per i soggetti pubblici interessati al trattamento dei dati personali effettuato per finalità previdenziali e per la gestione del rapporto di lavoro secondo, quanto stabilito dall'art. 111 del d.lgs. 196/2003.

IIª PARTE

INDICE:

Articolo 1 - Distribuzione dei compiti e delle responsabilità	6
Articolo 2 - Ricognizione dei dati personali e delle operazioni di trattamento	6
Articolo 3 - Analisi dei rischi	6
Articolo 4 - Misure minime di sicurezza	6
Articolo 5 - Criteri e modalità di salvataggio e ripristino dei dati	7
Articolo 6 - Pianificazione degli interventi formativi previsti	7

Allegati:

A - Strutture preposte ai trattamenti

B - Elenco dei trattamenti: Informazioni di base

C - Analisi dei rischi

Articolo 1 - Distribuzione dei compiti e delle responsabilità

La struttura amministrativa di Ateneo è quella approvata ai sensi del vigente Regolamento sull'ordinamento degli uffici e servizi, dal Consiglio di Amministrazione e riprodotta nell'Allegato A al presente documento.

La Direzione e la responsabilità di tipo amministrativo e tecnico è affidata al Direttore Amministrativo, al personale dirigenziale ed ai Responsabili di Servizio e di posizione organizzativa (Ufficio di Staff e Presidi di Facoltà e Dipartimento) individuati con formale provvedimento dal Consiglio di Amministrazione.

La Direzione e la responsabilità dei dati trattati nell'attività di ricerca è affidata ai Direttori di Dipartimento, ai Direttori dei Centri di ricerca e di servizio di Ateneo, ai Direttori dei Centri di ricerca e di servizio di Facoltà e di Dipartimento come indicato nell'allegato A al presente Regolamento.

Al personale sopra indicato verranno attribuite le responsabilità ed i compiti che il d.lgs. 196/2003 riconosce alla figura di responsabile (art. 29).

Articolo 2 - Ricognizione dei dati personali e delle operazioni di trattamento

Ferme restando le disposizioni del titolo VI, titolo VII e titolo VIII del d.lgs. 196/2003 i dati trattati, le operazioni effettuate, sono quelli riportate nell'allegato B al presente documento.

Articolo 3 - Analisi dei rischi

Il trattamento dei dati sensibili e giudiziari che sono gestiti esclusivamente su supporto cartaceo, avviene nel rispetto delle norme che definiscono l'entità e i tipi di dati trattati e le operazioni eseguibili.

I rischi dei dati personali riportati su supporto cartaceo e informatico sono la distruzione o la perdita anche accidentale e l'intrusione da parte di soggetti estranei non autorizzati ad introdursi nel trattamento.

Per i dati personali gestiti mediante strumenti elettronici valgono le misure indicate specificatamente nell'allegato C al presente documento.

Articolo 4 - Misure minime di sicurezza

Il titolare responsabile del trattamento definisce, nell'ambito delle rispettive competenze, così come individuate nei precedenti artt. 3, 4 e 5 della prima parte del presente atto, le misure minime di sicurezza previste dal d.lgs. 196/2003.

Contro i rischi di accesso abusivo ai dati si adottano le misure che consentano l'accesso ai dati esclusivamente ai dipendenti che hanno acquisito un'esperienza adeguata, ai quali sono state rese note la natura dei rischi e la responsabilità del trattamento.

L'incaricato è tenuto a custodire il materiale cartaceo riservato affinché sia escluso l'accesso non autorizzato, anche in occasione di temporanea assenza dalla postazione di lavoro.

I dati sulla salute del personale vengono conservati separatamente rispetto ad ogni altro dato personale, anche in riferimento ai fascicoli personali cartacei.

I dati personali riguardanti i lavoratori e prestatori d'opera sono custoditi in modo da garantire la loro riservatezza e, contemporaneamente, inibire l'accesso, l'utilizzazione, la comunicazione o la modifica da parte di personale non autorizzato.

I dati personali di tipo sensibile e giudiziario vengono custoditi in particolari archivi ad accesso selezionato, ciò in particolare avviene per i referti delle visite di controllo previste dal d.lgs. 626/94 e s.m.i.

Le procedure inerenti i dati personali sensibili e giudiziari sono assegnati ai dipendenti che offrono sul piano dell'esperienza ed affidabilità le necessarie garanzie.

Il personale incaricato della gestione di dati sensibili o di dati giudiziari procederà nel rispetto di dettagliate istruzioni, anche di tipo verbale. I dati in esame e le operazioni riepilogati nel prospetto si riferiscono ai dati inerenti la salute del lavoratore, e in relazione all'applicazione della legge sul lavoro dei disabili, sulla tutela della lavoratrice madre, la gestione delle deleghe sindacali e delle norme in materia di diritti sindacali in genere.

Il trattamento avrà ad oggetto unicamente i dati necessari alla instaurazione e gestione dei rapporti di lavoro di qualunque tipo e ad essa affini.

Accesso ed uso dei sistemi

1. Le unità disco (locali o di rete) sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia connesso all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
2. L'utente si connette alla rete interna tramite autenticazione univoca personale. Il titolare della password è tenuto a non rivelarla, dovendone avere la massima diligenza e preservandone la segretezza anche durante il momento della digitazione. Qualora l'utente prenda coscienza che taluno può aver visionato la digitazione o essere comunque a conoscenza della password, deve cambiarla immediatamente.
3. L'utente ha l'obbligo di cambiare la password ogni 6 mesi, in relazione alle misure di sicurezza minime per il trattamento dei dati sensibili.

Utilizzo supporti magnetici e dati

1. È fatto obbligo conservare, custodire e controllare i supporti informatici removibili affinché nessun soggetto terzo ne prenda visione o possesso.
2. Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso all'utente.

Trattamento senza l'impiego di strumenti elettronici

Qualora il trattamento abbia ad oggetto dati personali contenuti esclusivamente su supporti di tipo cartaceo, le misure di sicurezza vertono su disposizioni, anche di tipo verbale, che guidano gli operatori nel trattamento.

La sede degli uffici è sorvegliata durante le ore di chiusura e durante l'orario di apertura delle sedi di Ateneo il servizio di sorveglianza è normalmente assicurato dal personale ausiliario e dai dipendenti assegnati agli uffici.

Trattamenti con strumenti elettronici

I dati personali gestiti attraverso strumenti elettronici comportano l'assunzione di misure rivolte ad evitare l'accesso non autorizzato alle banche dati, alla rete e, in generale, ai servizi informatici.

Qualora il trattamento del dato venga assicurato da sistemi operativi esterni all'Amministrazione, si provvederà ad assumere con gli Enti convenzionati per la gestione esternalizzata un protocollo capace di assicurare le misure minime richieste dal codice.

Articolo 5 - Criteri e modalità di salvataggio e ripristino dei dati

L'utente dovrà farsi carico di effettuare una copia dei dati sul Server di Ateneo o sulla propria postazione (produttività individuale).

Il ripristino dei dati, a partire dalle copie giornaliere su nastro, sarà possibile per le informazioni residenti sui server centrali di Ateneo.

Articolo 6 - Pianificazione degli interventi formativi previsti

L'Amministrazione, nell'ambito del programma formativo annuale, prevede momenti di sensibilizzazione/formazione dedicati ad approfondire le problematiche applicative della normativa in materia di protezione dei dati personali, in relazione alla specifica natura dei dati raccolti e trattati all'interno dell'Ateneo.

Nell'ambito di tali iniziative, saranno altresì affrontati i temi riguardanti la responsabilità delle figure interessate al trattamento dei dati e le misure atte a garantire il corretto trattamento dei dati e la loro protezione, in particolare con riferimento ai dati sensibili e giudiziari.