UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA

REGOLAMENTO PER L'ATTUAZIONE DEL CODICE IN MATERIA DI DATI PERSONALI

Emanato con Decreto 11 febbraio 2005, n. 7445
Ultime modifiche emanate con Decreto 10 gennaio 2006, n. 9279
Entrate in vigore il 26 gennaio 2006

UFFICIO AFFARI GENERALI, ORGANI E RAPPORTI SSN
Via Ravasi, 2 – 21100 Varese (VA) – Italia
Tel. +39 033221 9034/9035/9044/9048/9052/9136 – Fax +39 0332 219039
Email: affari.generali@uninsubria.it - PEC: ateneo@pec.uninsubria.it
Web: www.uninsubria.it
P.I. 02481820120 - C.F. 95039180120
Chiaramente Insubria!

Piano I
Uff. 1.017 – 1.018

REGOLAMENTO PER L'ATTUAZIONE DEL CODICE IN MATERIA DI DATI PERSONALI

INDICE

PARTE I: PRINCIPI GENERALI 3
Art. 1 - Oggetto del Regolamento 3
Art. 2 - Definizioni 3
Art. 3 - Circolazione dei dati all'interno dell'Università 5
Art. 4 - Circolazione dei dati all'esterno dell'Università 5
Art. 5 - Diritto di accesso ai dati 6
PARTE II: I SOGGETTI 6
Art. 6 - Titolare, Responsabile ed Incaricato del trattamento dei dati, Incaricato della custodia delle parole chiave e Amministratore di sistema 6
Art. 7 - Responsabilità 7
PARTE III - IL TRATTAMENTO DEI DATI PERSONALI 8
Art. 8 - Modalità di raccolta e requisiti dei dati personali 8
Art. 9 - Notificazione al Garante 8
Art. 10 - Tipologie dei dati trattati dall'Università 8
Art. 11 - Informativa 9
Art. 12 - Diritti dell'interessato 9
Art. 13 - Forma della richiesta di comunicazione e diffusione dei dati 10
PARTE V – LA SICUREZZA DEI DATI 10
Art. 20 - Misure minime di sicurezza 10
Art. 21 - Misure idonee di sicurezza 10
Art. 22 - Documento Programmatico sulla Sicurezza 11
PARTE VI –DISPOSIZIONI TRANSITORIE E FINALI 11
Art. 23 - Disposizioni transitorie 11
Art. 24 - Disposizioni finali 11
Art. 25 - Entrata in vigore 11
ALLEGATO 1 12

PARTE I: PRINCIPI GENERALI

Art. 1 - Oggetto del Regolamento

1. Il presente Regolamento è emanato in attuazione del Decreto Legislativo 30 giugno 2003 n. 196 e disciplina il trattamento, la comunicazione e la diffusione da parte dell'Università degli Studi dell'Insubria dei dati personali, trattati sia con sistemi automatizzati che non automatizzati, per il perseguimento dei propri fini istituzionali.
2. Le disposizioni del presente Regolamento garantiscono il trattamento di informazioni a carattere personale, acquisite dall'Amministrazione Universitaria o ad essa rese, riguardanti persone fisiche o giuridiche, secondo criteri coerenti con la normativa in materia di protezione dei dati personali.
3. Sono esclusi dalla disciplina del presente Regolamento i trattamenti dei dati raccolti dal personale docente e ricercatore dell'Università per lo svolgimento della propria attività didattica e per finalità di ricerca esclusivamente individuali. Il personale docente e ricercatore dell'Università, comunque, si conformano al Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuato per scopi statistici e scientifici emanato dall'Autorità Garante per la protezione dei dati (G.U. n. 190 del 14 agosto 2004).
4. Sono altresì esclusi dalla disciplina del presente Regolamento i trattamenti dei dati sensibili e giudiziari che sono oggetto di altro specifico Regolamento di Ateneo, salvo per quanto prescritto dalle Linee guida per l'adozione delle misure minime di sicurezza (allegato 1 al presente Regolamento).

Art. 2 - Definizioni

1. Ai fini del presente Regolamento si applicano le definizioni elencate nel Decreto Legislativo 30 giugno 2003, n. 196. Si intende per:

Trattamento: Qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, 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 (art.4, c1,lett.a del D.Lgs. 196/2003).

Dato personale: 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 (art.4, c1,lett.b del D.Lgs. 196/2003).

Dati sensibili: 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 (art.4, c1,lett.d del D.Lgs. 196/2003).

Dati identificativi: I dati personali che permettono l'identificazione diretta dell'interessato (art.4, c1, lett.c del D.Lgs. 196/2003).

Dati giudiziari: I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313 in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi

	degli articoli 60 e 61 del codice di procedura penale (art.4, c1,lett.e del D.Lgs. 196/2003).
Dato anonimo:	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile, può essere trattato senza il consenso da parte dell'interessato (art.4, c1,lett.n del D.Lgs. 196/2003).
Titolare:	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(art.4, c1,lett.f del D.Lgs. 196/2003).
Responsabile:	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art.4, c1,lett.g del D.Lgs. 196/2003).
Incaricati:	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile(art.4, c1,lett.h del D.Lgs. 196/2003).
Interessato:	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (art.4, c1, lett.i del D.Lgs. 196/2003).
Comunicazione:	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art.4, c1,lett.l del D.Lgs. 196/2003).
Diffusione:	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art.4, c1, lett.m del D.Lgs. 196/2003).
Blocco:	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento (art.4, c1, lett.o del D.Lgs. 196/2003).
Banca di dati:	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (art.4, c1,lett.p del D.Lgs. 196/2003).
Garante	Autorità garante per la protezione dei dati personali istituita ai sensi dell'art. 30 della Legge 675/1996.
Misure minime:	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 (art.4, c3, lett.a del D.Lgs. 196/2003).
Strumenti elettronici:	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento (art.4, c3, lett.b del D.Lgs. 196/2003).
Sistema di autenticazione informatica:	L'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità o della dichiarazione di identità (art.4, c3, lett.c del D.Lgs. 196/2003).
Credenziali di autenticazione:	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati dal sistema di autenticazione informatica per la verifica dell'identità o di una dichiarazione di identità (art.4, c3, lett.d del D.Lgs. 196/2003).

Parola chiave:	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica (art.4, c3, lett.e del D.Lgs. 196/2003).
Profilo di autorizzazione:	L'insieme dei dati cui una persona può accedere, nonché dei trattamenti ad essa consentiti (art.4, c3, lett.f del D.Lgs. 196/2003).
Sistema di autorizzazione:	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 (art.4, c3, lett.g del D.Lgs. 196/2003).
Amministratori di sistema	I soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione (art. 1 c1 lett.c del DPR 318/99).
Documento programmatico sulla Sicurezza:	Documento che definisce, sulla base dell'analisi dei rischi, le misure di sicurezza da adottare a protezione dei dati sensibili e/o giudiziari trattati con l'ausilio di strumenti elettronici. Tale documento deve essere obbligatoriamente predisposto e revisionato con cadenza annuale entro il 31 marzo.
Scopi statistici	Le finalità di indagine statistica o di produzione di risultati statistici.
Scopi scientifici	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art. 3 - Circolazione dei dati all'interno dell'Università

1. Le disposizioni contenute negli articoli che seguono s'intendono riferite al trattamento, alla diffusione ed alla comunicazione dei dati a terzi. L'accesso ai dati personali da parte delle strutture amministrative, di servizio, didattiche e scientifiche e dei dipendenti dell'Università è limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali ed è ispirato al principio della libera circolazione delle informazioni.
2. L'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università deve essere debitamente motivato e connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, e viene valutato in via diretta e senza formalità nella misura necessaria al perseguimento dell'interesse istituzionale. Qualora invece l'accesso sia giustificato per un utilizzo ulteriore e/o diverso dei dati, i soggetti già indicati devono presentare esplicita e formale richiesta; questa ultima viene esaminata dal Responsabile del trattamento dei dati, e l'autorizzazione viene concessa o negata a seconda che il fine della richiesta rientri o meno nell'attività istituzionale dell'Università. Il richiedente deve adottare tutte le misure necessarie a garantire la sicurezza dei dati a lui trasmessi.
3. Ai fini dell'accesso ai dati sono equiparati alle strutture dell'Università gli organismi sindacali, gli organismi di controllo e di valutazione ed ogni altro organo a cui espresse disposizioni normative affidano tali compiti.

Art. 4 - Circolazione dei dati all'esterno dell'Università

1. Al fine di favorire l'inserimento nel mondo del lavoro e della ricerca degli studenti che hanno conseguito il titolo conclusivo dei corsi di studi di ogni tipologia prevista nel proprio ordinamento didattico, l'Università può comunicare e diffondere all'esterno i dati personali attinenti alla carriera degli studenti medesimi, alle loro competenze ed aspirazioni professionali, su richiesta di soggetti pubblici, aziende private, associazioni di categoria e altri soggetti privati ovvero di propria iniziativa, anche mediante inserimento in sito Internet o in altri circuiti informativi.

2. L'Università avrà cura di chiedere il preventivo consenso scritto degli studenti interessati, previa informativa ai sensi dell'art. 13 del Decreto Legislativo 30 giugno 2003, n. 196.

Art. 5 - Diritto di accesso ai dati

1. L'esercizio del diritto di accesso è subordinato alla sussistenza di un interesse per la tutela di situazioni giuridicamente rilevanti.
2. Oggetto del diritto di accesso è il documento amministrativo. Come stabilito dall'art. 59 del Decreto Legislativo 30 giugno 2003, n. 196 il diritto all'accesso a documenti amministrativi contenenti dati personali resta disciplinato dalla Legge 7 agosto 1990, n. 241 e successive modificazioni ed integrazioni.
3. L'esercizio del diritto d'accesso, se implica la comunicazione di dati personali di terzi, deve essere limitato unicamente ai dati necessari a soddisfare il diritto stesso.
4. Ai sensi dell'art. 60 del Decreto Legislativo n. 196/2003, quando la richiesta di accesso concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito solo se il diritto sottostante che il terzo intende far valere, sulla base del materiale documentale al quale chiede di accedere, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

PARTE II: I SOGGETTI

Art. 6 - Titolare, Responsabile ed Incaricato del trattamento dei dati, Incaricato della custodia delle parole chiave e Amministratore di sistema

1. L'Università degli Studi dell'Insubria è Titolare del trattamento dei dati personali, ivi compresi i dati contenuti nelle banche di dati, automatizzate o cartacee, detenuti dall'Università.
2. Il Titolare predispone ed approva il documento programmatico sulla sicurezza, organizza le attività di vigilanza e di controllo, verifica la rispondenza dei trattamenti effettuati alle modalità prescritte dal Regolamento ed attua gli eventuali adattamenti.
3. Nell'ambito dell'Università, il Responsabile del trattamento dei dati personali e delle banche dati è il responsabile della struttura all'interno della quale i dati personali o le banche dati sono gestiti per le finalità istituzionali della rispettiva unità organizzativa.
4. Sono individuati a tal fine le seguenti strutture con i rispettivi responsabili:

STRUTTURE	RESPONSABILI DEL TRATTAMENTO
Facoltà	Presidi di Facoltà
Dipartimento, Centri di servizio e Centri Speciali	Direttori di Dipartimento,dei Centri di servizio e dei Centri Speciali
Scuole di Specializzazione	Direttori delle Scuole di Specializzazione
Direzione Amministrativa e Uffici di Staff della Direzione amministrativa	Direttore Amministrativo
Segreteria del Rettore	Responsabile dell'Ufficio

Uffici di Staff del Rettore	Rettore
Segreteria del Rettore Vicario e della vice Direzione amministrativa	Responsabile dell'Ufficio
Settori dell'Amministrazione Centrale	Responsabili di Settore
Ufficio speciale per l'edilizia universitaria	Responsabile dell'Ufficio

5. Qualora i dati o le banche dati siano gestiti su sistemi informatici amministrati dal SIC (Centro Sistemi informativi e comunicazione) o da altre strutture dell'Università, il Direttore del SIC o della struttura che amministra il sistema è individuato quale Amministratore di Sistema; lo stesso soggetto è altresì responsabile del trattamento dei dati limitatamente alle operazioni connesse con l'esercizio dei sistemi informatici contenenti i dati o le banche dati.
6. Il Titolare, nella persona del Rettore pro-tempore, può comunque designare, con provvedimento formale, uno o più responsabili del trattamento dei dati diversi dai soggetti sopra indicati.
7. I Responsabili, sotto il diretto controllo del Titolare del trattamento, assicurano l'esercizio delle istruzioni impartite dal Titolare del trattamento per l'attuazione della Decreto Legislativo 30 giugno 2003, n. 196 anche tramite verifiche periodiche. Inoltre, garantiscono l'attuazione delle misure di sicurezza dei dati e del Documento Programmatico sulla Sicurezza di cui ai successivi artt. 21 e 22 del presente Regolamento, istruiscono e controllano i dipendenti Incaricati del trattamento dei dati.
8. I Responsabili del trattamento provvedono ad identificare e segnalare al Titolare eventuali ulteriori trattamenti di dati, diversi da quelli sensibili e giudiziari già oggetto di specifico regolamento di Ateneo, che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura degli stessi, alle modalità o agli effetti del trattamento.
9. I Responsabili del trattamento designano, con propri atti scritti, gli Incaricati del trattamento dei dati operanti all'interno della struttura di competenza. Ciascun Responsabile del trattamento provvede, altresì, alla custodia delle parole chiave degli Incaricati dallo stesso designati.
10. Gli Incaricati devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del Titolare o del Responsabile sotto la cui diretta autorità operano.

Art. 7 - Responsabilità

1. Il soggetto che richiede, riceve, tratta, o semplicemente ha notizia di dati è vincolato al rispetto del segreto d'ufficio di cui all'art. 15 del D.P.R. 10 Gennaio 1957 n. 3, come sostituito dall'art. 28 della Legge 7 Agosto 1990 n. 241.
2. Le attività di trattamento dei dati personali sono state equiparate alle attività pericolose, pertanto, chiunque cagioni un danno ad altri per effetto delle operazioni di trattamento (art. 15 del D. Decreto Legislativo 30 giugno 2003, n. 196) è tenuto al risarcimento del danno ai sensi dell'articolo 2050 del codice civile.
3. Le responsabilità dei soggetti di cui all'art. 6 c4 comprendono anche quella relativa alla mancata vigilanza sull'attività degli incaricati al trattamento dei dati, all'omessa o inidonea informativa fornita all'interessato.
4. La responsabilità, anche penale, espressamente prevista dal Decreto Legislativo 30 giugno 2003, n. 196 per un eventuale utilizzo illecito o non corretto dei dati personali conosciuti o per la mancata adozione delle misure di sicurezza (artt. 33-36 del Decreto Legislativo 30 giugno 2003, n. 196 e Di-

sciplinare Tecnico in materia di misure minime di sicurezza, allegato allo stesso) è a carico della singola persona, titolare, responsabile o incaricato, cui l'uso illegittimo sia riferibile.

PARTE III - IL TRATTAMENTO DEI DATI PERSONALI

Art. 8 - Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:
   a. trattati in modo lecito e secondo correttezza;
   b. raccolti e registrati per scopi determinati, espliciti e legittimi, utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
   c. esatti e, se necessario, aggiornati;
   d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
   e. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario per gli scopi per i quali i dati sono stati raccolti o successivamente trattati.
2. Il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati e può essere effettuato, ai sensi dell'art. 99 c2 del Decreto Legislativo 30 giugno 2003, n. 196, anche oltre il periodo necessario a questi ultimi scopi.

Art. 9 - Notificazione al Garante

1. Il Titolare, prima di procedere ad un nuovo trattamento di dati personali, provvederà, ove ne ricorrano le condizioni, a darne notificazione al Garante nei termini previsti dalla legge.
2. Per consentire al Titolare la notificazione delle banche di dati prevista dal Decreto Legislativo 30 giugno 2003, n. 196 chi intende procedere, nell'ambito delle funzioni universitarie, ad un nuovo trattamento di dati personali per i quali è previsto l'obbligo della notificazione al Garante deve comunicarlo al responsabile della struttura organizzativa, tra quelle indicate al precedente art. 6 c4 del presente Regolamento. La comunicazione contiene:
   a. le finalità e le modalità del trattamento;
   b. la natura dei dati, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono;
   c. l'ambito di comunicazione e di diffusione dei dati;
   d. gli eventuali trasferimenti di dati previsti verso Paesi non appartenenti all'Unione Europea o, qualora si tratti di dati sensibili e di dati relativi ai provvedimenti di cui all'art. 686 c.p.p., fuori del territorio nazionale;
   e. una descrizione delle misure di sicurezza adottate;
   f. l'eventuale connessione con altri trattamenti o banche di dati, e comunque ogni altra informazione utile al Titolare per procedere alla notificazione di cui all'art. 37 del Decreto legislativo 30 giugno 2003, n. 196.

Art. 10 - Tipologie dei dati trattati dall'Università

1. Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dal Decreto Legislativo 30 giugno 2003, n. 196 e dal presente Regolamento.

2. L'Università degli Studi dell'Insubria è un'istituzione pubblica di alta cultura che ha per finalità lo sviluppo del sapere critico e della sua trasmissione. L'Università opera per attuare il diritto allo studio con particolare riguardo ai capaci e meritevoli, anche di concerto con gli enti competenti in materia. Favorisce la qualità e l'efficacia dell'attività di formazione degli studenti e ne cura la preparazione professionale. Nel perseguimento dei suoi fini, assicura il rispetto della libertà di ricerca e della libertà di insegnamento costituzionalmente protetti. Individua, coordina e predispone i mezzi materiali e finanziari a ciò necessari, in rapporto alle esigenze ed alle risorse. L'Università garantisce il raggiungimento delle proprie finalità istituzionali per mezzo delle sue strutture didattiche, ed attraverso la conclusione di apposite convenzioni con istituzioni ed organismi di alta cultura nazionali ed esteri, operanti nel campo della didattica e della ricerca, e con enti pubblici e privati.
3. Per il perseguimento dei propri fini istituzionali l'Università tratta principalmente le seguenti tipologie di dati personali:
    a. dati relativi al personale dipendente ed a contratto;
    b. dati relativi a studenti, inclusi coloro che hanno già terminato gli studi;
    c. dati relativi al personale operante a vario titolo nell'Università (borsisti, tirocinanti, visitatori ecc.);
    d. dati raccolti per fini amministrativi e contabili;
    e. dati raccolti per fini di didattica e ricerca.

Art. 11 - Informativa

1. L'interessato deve essere debitamente informato, prima del trattamento dei dati personali, circa:
    a. le finalità e le modalità del trattamento cui sono destinati i dati richiesti;
    b. la natura obbligatoria o facoltativa del conferimento di dati richiesti;
    c. i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
    d. i diritti di cui all'art. 7 del Decreto Legislativo 30 giugno 2003, n. 196;
    e. i dati relativi al titolare e, se designato, del responsabile.
2. L'informativa può essere resa individualmente, attraverso modalità orali o scritte, oppure collettivamente, mediante informative di massa od annunci sulle pagine Web.

Art. 12 - Diritti dell'interessato

1. Il soggetto i cui dati sono contenuti in una banca di dati ha il diritto di ottenere, senza ritardo, ai sensi dell'art. 7 del Decreto Legislativo 30 giugno 2003, n. 196:
    a. la conferma dell'esistenza o meno di trattamenti che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento;
    b. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
    c. l'aggiornamento, la rettificazione, ovvero, qualora vi abbia interesse, l'integrazione dei dati;
    d. l'attestazione che le operazioni di cui alle lett. b e c sono state portate a conoscenza dei terzi.
2. L'interessato ha, inoltre, il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta, l'interessato può esercitare tali diritti con una richiesta scritta al responsabile della banca dati.
3. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Art. 13 - Forma della richiesta di comunicazione e diffusione dei dati

1. La comunicazione e la diffusione dei dati sono permesse quando:
   a. siano previste da una norma di legge o di regolamento;
   b. siano necessarie per finalità di ricerca scientifica o di statistica, e si tratti di dati anonimi;
   c. siano richieste dai soggetti di cui all'art. 25, c2 del Decreto Legislativo 30 giugno 2003, n. 196 per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati;
   d. sia stata espressamente autorizzata dagli interessati.
2. Al fine di ottenere la comunicazione dei dati, i richiedenti presentano una richiesta scritta e motivata al Titolare o al Responsabile del trattamento, indicando oltre che i dati cui essa fa riferimento:
   a. il nome, la denominazione o la ragione sociale;
   b. le finalità e le modalità di utilizzo dei dati richiesti. I dati vengono rilasciati a condizione che il richiedente si impegni ad utilizzarli esclusivamente per le finalità e nell'ambito delle modalità indicate, e ad adottare tutte le misure necessarie a garantirne la sicurezza.
3. L'Università, dopo avere valutato che la diffusione e la comunicazione dei dati sono compatibili con i propri fini istituzionali, provvede alla trasmissione dei dati stessi nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.
4. Nei limiti di cui all'art. 19, c2, del Decreto Legislativo 30 giugno 2003, n. 196 le richieste provenienti da soggetti pubblici, esclusi gli enti pubblici economici, finalizzate alla comunicazione dei dati sono soddisfatte quando necessarie al perseguimento dei fini istituzionali dell'ente richiedente.

PARTE V – LA SICUREZZA DEI DATI

Art. 20 - Misure minime di sicurezza

1. Il Titolare ed i Responsabili del trattamento dei dati provvedono, per quanto di loro competenza così come indicato al c4 dell'art. 6 del presente Regolamento, in relazione alla disciplina disposta agli artt. 33, 34 35 e 36 del Decreto Legislativo 30 giugno 2003, n. 196, all'adozione delle misure minime di sicurezza secondo le linee guida allegate al presente Regolamento al fine di prevenire:
   a. i rischi di distruzione, perdita anche accidentale di dati o danneggiamento delle banche dati o dei locali ove esse sono custodite;
   b. l'accesso non autorizzato ai dati stessi;
   c. modalità di trattamento dei dati non consentite rispetto alla legge o al presente Regolamento;
   d. modalità di trattamento dei dati non conformi rispetto alle finalità della raccolta.

Art. 21 - Misure idonee di sicurezza

1. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze rese disponibili dal 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. Al riguardo l'Università predispone l'adozione delle misure idonee previste ai sensi dell'art. 31 del Decreto Legislativo 30 giugno 2003 n. 196.

Art. 22 - Documento Programmatico sulla Sicurezza

1. Nel caso di trattamento di dati sensibili e giudiziari, deve essere predisposto un Documento Programmatico sulla Sicurezza ai sensi dell'art. 34 lett.) del Decreto Legislativo 30 giugno 2003, n. 196 e del punto 19 del Disciplinare Tecnico in materia di misure minime di sicurezza allo stesso allegato.
2. Il Documento Programmatico sulla Sicurezza previsto dal decreto ha lo scopo di individuare tutte le misure di protezione necessarie a garantire la sicurezza dei dati sensibili e giudiziari che debbono essere adottate in via preventiva da tutti coloro che effettuano operazioni di trattamento degli stessi.
3. Il Documento Programmatico sulla Sicurezza deve essere approvato, previo parere del Comitato Tecnico Scientifico del Centro SIC, dal Senato Accademico dell'Università e deve essere conosciuto ed applicato dall'Ateneo. Il Documento Programmatico sulla Sicurezza, inoltre, deve essere revisionato entro il 31 marzo di ciascun anno.

PARTE VI –DISPOSIZIONI TRANSITORIE E FINALI

Art. 23 - Disposizioni transitorie

1. In sede di prima applicazione del presente Regolamento, le misure di sicurezza di cui di cui all'art. 21 ed il Documento Programmatico sulla Sicurezza di cui all'art. 23 del presente Regolamento saranno adottate entro il 31 marzo 2005.

Art. 24 - Disposizioni finali

1. Per quanto non previsto nel presente Regolamento, si applicano le disposizioni del Decreto Legislativo 30 giugno 2003 n. 196 e le successive modificazioni ed integrazioni.

Art. 25 - Entrata in vigore

2. 1. Il presente Regolamento entra in vigore contestualmente alla pubblicazione del decreto rettorale di emanazione all'albo dell'Università.

ALLEGATO 1

LINEE GUIDA PER L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA

Vengono riportati nel seguito le linee guida definite dall'Università sulla base degli artt. 33, 34, 35 e 36 del Decreto Legislativo 196/2003 e delle disposizioni del Disciplinare Tecnico in tema di misure minime allo stesso allegato, al fine di assicurare un livello minimo di protezione ai dati, alle informazioni ed alle risorse informatiche gestite sia su formato elettronico che cartaceo.

Regole generali

Personale autorizzato al trattamento dei dati

DESIGNAZIONE DEGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI	Devono essere designati per iscritto dai Responsabili del trattamento, gli Incaricati del trattamento cartaceo ed elettronico dei dati personali. Tale designazione deve individuare puntualmente l'ambito del trattamento consentito (banche dati, operazioni effettuabili e durata dell'incarico).
AUTORIZZAZIONE AL TRATTAMENTO DEI DATI SENSIBILI E/O GIUDIZIARI	Nel caso di trattamento cartaceo od elettronico di dati sensibili e/o giudiziari, gli Incaricati devono essere anche essere autorizzati per iscritto.

Trattamento di dati idonei a rivelare stato di salute e vita sessuale

MODALITÀ DI TRATTAMENTO	Le modalità di trattamento di dati idonei a rivelare stato di salute e vita sessuale contenuti in elenchi, registri o banche di dati devono consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati

Trattamento elettronico dei dati

Profili di autorizzazione

INDIVIDUAZIONE DEI PROFILI	I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, devono essere individuati dal Responsabile del trattamento dei dati e configurati dall'Amministratore di sistema anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Per quanto attiene il trattamento dei dati sensibili e/o giudiziari, la lista degli Incaricati può essere redatta dai Responsabili del trattamento dei dati anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
AGGIORNAMENTO DEI PROFILI	Periodicamente, e comunque almeno annualmente, il Responsabile del trattamento dei dati deve verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. In caso di: ▪ cambio di ruolo (variazione dei privilegi); ▪ dimissioni/licenziamento di un incaricato del trattamento (revoca del profilo); ▪ assenza prolungata dal luogo di lavoro (sospensione del profilo);

	il Responsabile del trattamento deve darne immediata comunicazione all'Amministratore di sistema che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione. Per quanto attiene il trattamento dei dati sensibili e/o giudiziari, l'aggiornamento deve avvenire almeno con cadenza annuale dall'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.

Credenziali di autenticazione

CREDENZIALI DI AUTENTICAZIONE	Le credenziali di autenticazione devono consistere: ▪ in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo; ▪ oppure in un dispositivo di autenticazione in possesso ad uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave; ▪ oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE	Ad ogni Incaricato devono essere assegnate o associate individualmente una o più credenziali per l'autenticazione. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
DISATTIVAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE	Le credenziali di autenticazione non utilizzate da almeno 6 (sei) mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali devono essere disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. In entrambe i casi il Responsabile del trattamento deve darne immediata comunicazione all'Amministratore di sistema che provvederà a disattivare il profilo del soggetto in questione.
LUNGHEZZA DELLA PAROLA CHIAVE	La parola chiave, quando è prevista dal sistema di autenticazione: ▪ deve essere composta da almeno 8 (otto) caratteri; ▪ oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
FORMATO DELLA PAROLA CHIAVE	La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato, quindi non deve derivare dal nome utente o dai dati personali dell'utente.
MODIFICA DELLA PAROLA CHIAVE	La parola chiave deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni 6 (sei) mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni 3 (tre) mesi.

ISTRUZIONI AGLI INCARICATI	Nome utente e password sono strettamente personali e l'incaricato è tenuto: ▪ a non comunicare a terzi le password; ▪ a non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi; ▪ ad attenersi a tutte le indicazioni contenute nelle istruzioni fornite dal Titolare o dal Responsabile. Devono essere impartite istruzioni agli incaricati attraverso le quali è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. Devono essere impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Controllo degli accessi

SISTEMA DI CONTROLLO ACCESSI	I dati personali, sensibili e/o giudiziari devono essere protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale. I server di rete e tutte le postazioni lavorative (Personal Computer) devono essere protetti contro il rischio di intrusione mediante l'attivazione di idonei strumenti elettronici. Deve, quindi, essere presente un sistema di controllo degli accessi basato principalmente sulle seguenti politiche di gestione delle password: ▪ tutte le postazioni di lavoro utilizzate dall'università sono protette da una password di accesso; ▪ la password di accesso va modificata con cadenza definita sulla base della tipologia di dati trattati; ▪ ai fini dell'assistenza sistemistica, la password di accesso può venire comunicata dagli Incaricati all'operatore, e sostituita al termine dell'intervento.
SISTEMI ANTINTRUSIONE	Per proteggere l'accesso da Internet alla LAN universitaria deve essere attivato un sistema antintrusione. Tale sistema deve essere configurato in modo da impedire l'accesso alla rete dall'esterno salvo se richiesto da alcuni servizi conosciuti e controllati.
ISTRUSIONI AGLI INCARICATI	Devono essere impartite idonee istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati.

Sistema antivirus

SISTEMA ANTIVIRUS	I dati personali, sensibili e/o giudiziari devono essere protetti contro il rischio di distruzione o perdita anche accidentale. I server di rete e tutte le postazioni lavorative (Personal Computer) devono essere protetti dall'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di sistemi antivirus aggiornati almeno ogni sei mesi.

Aggiornamento dei programmi

GESTIONE DEI PROGRAMMI	Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne i difetti, devono essere effettuati dall'Amministratore di sistema ogniqualvolta la casa produttrice rilascia un aggiornamento o almeno ogni sei mesi.

Sistema di back up dei dati

BACKUP DEI DATI	Deve essere attivato un sistema di backup giornaliero di tutti i dati personali presenti sui server, ed individuato uno o più Incaricati autorizzati all'effettuazione delle operazioni di backup sulla base di una procedura formalizzata per iscritto. Laddove il backup venga effettuato localmente nell'ambito dell'ufficio, gli Incaricati devono effettuano le seguenti operazioni: ▪ esecuzione settimanale del backup, eventualmente attraverso procedure automatiche; ▪ verifica almeno della corretta esecuzione dei backup; ▪ mantenimento di un elenco dei backup effettuati; ▪ archiviazione sicura dei supporti.
CONSERVAZIONE DEI SUPPORTI	I supporti utilizzati per le attività di Backup e Restore delle informazioni e delle applicazioni, devono essere tenuti in cassetti/armadi ignifughi muniti di serratura. I cassetti/armadi ignifughi devono essere posti in locali diversi dalla sala ove risiedono i server di rete o i personal computer.
ISTRUZIONI AGLI INCARICATI	Devono essere impartite istruzioni organizzative e tecniche agli Incaricati: ▪ che prevedono il salvataggio dei dati con frequenza almeno settimanale, laddove venga eseguito localmente; ▪ per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati.

Utilizzo e riutilizzo dei supporti di memorizzazione

RIUTILIZZO DEI SUPPORTI	I supporti rimovibili contenenti dati personali, sensibili e/o giudiziari possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili. Periodicamente i supporti di memorizzazione devono essere testati e verificati attraverso l'utilizzo di appositi strumenti atti ad accertare l'integrità dei dati registrati.
DISTRUZIONE DEI SUPPORTI	I supporti rimovibili contenenti dati sensibili e/o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili.

Ripristino dei dati

RIPRISTINO DEI DATI	Devono essere adottate idonee misure tecnologiche ed organizzative atte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici utili ai fini del loro utilizzo.
DANNEGGIAMENTO DELL'HARDWARE	Ai fini della conformità al D. Lgs. 196/2003, nell'eventualità che si danneggino in modo disastroso uno o più componenti hardware si dovrà intervenire tempestivamente per ripristinare i dati e i servizi nel più breve tempo possibile prevedendo: ▪ un eventuale spostamento temporaneo dei servizi non operativi su un altro Server, tenendo in considerazione i tempi e gli oneri di un tale intervento; ▪ l'attivazione di un contratto di assistenza tecnica che contempli la sostituzione delle parti guaste o difettose da parte del fornitore, ed il ripristino dei sistemi entro tempi prestabiliti; ▪ la sostituzione immediata delle parti danneggiate se presenti in Università come parte di

	ricambio, oppure acquisto delle parti presso il produttore.
TEMPI DI RIPRISTINO	Nel caso di trattamento di dati personali, il loro ripristino deve avvenire in tempi certi ed utili all'assolvimento degli obblighi di: ▪ evasione senza ritardo delle richieste avanzate dagli Interessati nell'esercizio dei propri diritti; ▪ evasione senza ritardo delle eventuali richieste di informazioni od di effettuazione di controlli ed accessi avanzata dall'Autorità Garante per la protezione dei dati. Nel caso di trattamento di dati sensibili e/o giudiziari il ripristino deve avvenire in tempi certi compatibili con i diritti degli interessati e non superiori a 7 (sette) giorni.

Outsourcing delle attività di trattamento

NOMINA DEL RESPONSABILE ESTERNO	Nel caso di affidamento a terzi delle attività di trattamento dei dati, questi ultimi devono essere formalmente nominati Responsabili del trattamento e devono esserne specificati i compiti e responsabilità.
CRITERI NELLA SCELTA DEL RESPONSABILE	E' possibile nominare Responsabili del trattamento dei dati in outsourcing solo quei soggetti terzi che abbiano i requisiti di esperienza, capacità ed affidabilità previsti all'art. 29 dal Decreto legislativo 196/2003.
VERIFICHE DI CONFORMITÀ	Il Titolare, anche avvalendosi dell'Amministratore di sistema, vigila, anche tramite verifiche periodiche, sulla puntuale osservanza da parte del Responsabile del trattamento dei dati in outsourcing del rispetto degli obblighi di sicurezza.

Trattamento cartaceo dei dati

Accesso agli atti ed ai documenti

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI	In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, ogni incaricato del trattamento dei dati operante nell'azienda, può accedere soltanto agli archivi relativi alle banche dati di tipo cartaceo per le quali ha ricevuto l'autorizzazione al trattamento dal Responsabile del trattamento dei dati.
ACCESSO AGLI ARCHIVI CONTENENTI DATI SENSIBILI O GIUDIZIARI	L'accesso agli archivi cartacei contenti dati sensibili e/o giudiziari: ▪ deve essere controllato; ▪ le persone ammesse dopo l'orario di chiusura sono identificate e registrate; ▪ se gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.
SMALTIMENTO DELLA CARTA	In fase di smaltimento dei rapporti cartacei deve essere vietato agli incaricati di lasciare integri i documenti contenenti dati personali. Tale divieto è maggiormente avvertito nel caso di documenti contenenti dati sensibili e/o giudiziari. Al riguardo risulta opportuno munirsi di appositi strumenti disintegratori. Deve anche essere prevista una procedura per l'eventuale riutilizzo della carta.

Custodia e controllo degli atti e dei documenti

COMUNICAZIONE DI ATTI E DOCUMENTI CONTENETI DATI PERSONALI, SENSIBILI E/O GIUDIZIARI	I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'Università.
CUSTODIA E CONTROLLO DI DOCUMENTI CONTENETI DATI SENSIBILI E/O GIUDIZIARI	Tutti i dati sensibili e/o giudiziari trattati manualmente devono essere protetti durante tutte le fasi di lavorazione e durante il loro ciclo di vita, dall'acquisizione all'eventuale distruzione, assicurandone costantemente la custodia e il controllo. Il trattamento dei documenti contenenti dati sensibili e/o giudiziari se affidati agli incaricati sono controllati e custoditi dagli incaricati stessi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate. Nel caso le informazioni cartacee debbano essere inserite in un elaboratore, la prassi operativa deve essere tale da garantire che i tabulati stampati non rimangano incustoditi e vengano immediatamente ritirati. Qualsiasi variazione di ubicazione dei dati o introduzione di nuovi tipi di dati sensibili e/o giudiziari deve essere tempestivamente comunicata al Responsabile del trattamento dei dati di competenza.
ISTRUZIONI SCRITTE AGLI INCARICATI	Devono essere impartite dai Responsabili del trattamento idonee istruzioni agli incaricati finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Devono essere fornite agli incaricati istruzioni opportune per non lasciare incustoditi gli atti e i documenti contenenti dati sensibili e/o giudiziari. Il personale deve essere adeguatamente formato sulle procedure e sulle modalità di organizzazione degli archivi cartacei.