

Emanato con D.R. n. 3631-2005 del 24.11.2005 - prot. n. 41764

Modificato con D.R. n. 1189-2008 del 14.04.2008 - prot. n. 17768

Regolamento in Materia di Trattamento, Comunicazione e Diffusione dei Dati Personali in possesso dell'Università degli Studi dell'Aquila

PARTE I GENERALITA'

Art. 1 Ambito di applicazione

1. L'Università provvede al trattamento, alla diffusione e alla comunicazione dei dati nell'ambito del perseguimento dei propri fini istituzionali.
2. Esula dalla disciplina del presente regolamento il trattamento dei dati raccolti dal personale docente e ricercatore dell'Università per lo svolgimento della propria attività didattica e per finalità di ricerca esclusivamente individuali.

Art. 2 Definizioni

Ai fini del presente regolamento ed in accordo al D. Lgs 30 giugno 2003 n.196 si intende per:

- **decreto:** il D. Lgs 30 giugno 2003 n.196;
- **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 dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- **responsabile:** la persona fisica, la persona giuridica, la pubblica amministrazione, e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento dei dati personali;
- **incaricati:** le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- **interessati:** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- **trattamento:** 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 dati;
- **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;

- **diffusione:** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **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 identificativo personale;
- **dati identificativi:** i dati personali che permettono l'identificazione diretta dell'interessato;
- **dati sensibili:** i dati personali atti a rilevare 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 rilevare lo stato di salute e la vita sessuale;
- **dati giudiziari:** i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, 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;
- **dato anonimo:** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- **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 (di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta);
- **archivio/banca dati:** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Art. 3 Titolari, responsabili ed incaricati

1. L'Università degli Studi dell' Aquila è titolare dei dati personali detenuti dall'Università stessa, raccolti o no in banche di dati, automatizzate o cartacee.
2. Il titolare individua i responsabili per il trattamento dei dati personali nelle figure dei responsabili delle diverse strutture amministrative, didattiche, di ricerca e di servizio, e i responsabili informatici:
 - a) il Coordinatore dell'Area Gestione dei Servizi Informatici, quale *Responsabile Informatico per l'Amministrazione Centrale e per le banche dati delle Facoltà del Polo Centro*;
 - b) il Coordinatore dell'Area Gestione dei Laboratori Scientifici e Didattici ad Indirizzo Informatico Polo Coppito, *quale Responsabile Informatico e per le banche dati delle Facoltà del Polo di Coppito*;

- c) il Coordinatore dell'Area Gestione dei Laboratori Scientifici e Didattici ad Indirizzo Informatico Polo Roio, *quale Responsabile Informatico e per le banche dati delle Facoltà del Polo di Roio;*”;
- d) I Direttori di Dipartimento *quali Responsabili e per le banche dati dei propri Dipartimenti;*”;
3. Il titolare può designare quali responsabili del trattamento altri soggetti, rispetto a quelli individuati al comma 2, anche estranei all'Ateneo.
4. Ciascun responsabile individua gli incaricati del trattamento dei dati all'interno delle singole strutture.
5. Gli incaricati, di cui al comma 4, svolgono le operazioni materiali inerenti al trattamento, operando sotto la diretta responsabilità del responsabile.
6. Titolare - E' compito del Titolare:
- rilevare le banche dati presenti, cartacee e/o elettroniche (ivi compresi gli archivi residenti su PC) e la relativa ubicazione (sedi, uffici, ..), classificando le informazioni in esse contenute (dati personali, sensibili, giuridici, anonimi), individuando i relativi trattamenti dei dati, i compiti e le responsabilità delle strutture preposte ai trattamenti, l'analisi dei rischi che incombono sui dati e le misure di sicurezza adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità; si consulti il Disciplinare Tecnico, Allegato B del Decreto, per ulteriori dettagli e si utilizzi, per la ricognizione, il documento messo a disposizione dall'Amministrazione;
 - effettuare, ove necessario, le notifiche al Garante;
 - individuare e nominare per iscritto i Responsabili del trattamento dei dati, dettagliando i relativi compiti e fornendo specifiche istruzioni sulle modalità di trattamento dei dati nel rispetto della normativa vigente in tema di privacy e sicurezza, con particolare riferimento all'adozione delle misure di sicurezza indicate nel decreto;
 - individuare e nominare per iscritto Responsabili anche eventuali soggetti giuridici esterni, come ad esempio nel caso di Ditte che curano servizi di manutenzione, consulenza, outsourcing, dettagliando i relativi compiti e fornendo specifiche istruzioni sulle modalità di trattamento dei dati nel rispetto della normativa vigente in tema di privacy e sicurezza; riportare, inoltre, nei contratti di fornitura/servizi un'apposita clausola che ne definisce i compiti e le responsabilità per le violazioni;
 - predisporre/aggiornare il documento programmatico sulla sicurezza di competenza in tempo utile per la relativa presentazione nella relazione accompagnatoria a ciascun bilancio di esercizio (31 marzo di ogni anno) e comunque entro il termine indicato dall'Amministrazione;
 - provvedere agli obblighi di informativa e, ove necessario, di richiesta di consenso verso l'interessato;
 - vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni e delle proprie istruzioni.7. In sede di prima applicazione del presente regolamento il titolare è tenuto a predisporre, previo censimento delle banche di dati esistenti presso le strutture, il documento programmatico per la sicurezza (DPS).

8. Annualmente il titolare è tenuto ad effettuare un aggiornamento di tale documento.
9. Responsabili - Ai fini dell'applicazione del D.Lgs 196/2003 sono responsabili dei dati personali detenuti dagli uffici di competenza:
 - a) i Presidi delle Facoltà;
 - b) i Direttori di Dipartimento;
 - c) il Dirigente del Dipartimento 1 (Ricerca e trasferimento tecnologico - RESMAN);
 - d) il Dirigente del Dipartimento 2 (Affari generali di Ateneo – AGENA);
 - e) il Direttore Amministrativo per il Dipartimento 3 (Didattica –DIDA) e per le strutture dell'amministrazione centrale, le Biblioteche di polo, il Centro linguistico ed ECDL
 - f) il Rettore per gli uffici di supporto alla governance di Ateneo e gli organi non riconducibili ai precedenti responsabili (ad esempio: il Nucleo di Valutazione, Collegio dei Revisori dei conti...)
 - g) il Delegato del Rettore per il Polo di Sulmona;
 - h) il Delegato del Rettore per il Polo di Avezzano.

E' compito dei Responsabili:

- rispettare ed applicare le disposizioni del Titolare;
- collaborare con il titolare nella rilevazione delle banche dati presenti, cartacee e/o elettroniche (ivi compresi gli archivi residenti su PC) e la relativa ubicazione (sedi, uffici, ..), classificando le informazioni in esse contenute (dati personali, sensibili, giuridici, anonimi), individuando i relativi trattamenti dei dati, i compiti e le responsabilità delle strutture preposte ai trattamenti, l'analisi dei rischi che incombono sui dati e le misure di sicurezza adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità; si consulti il Discipinare Tecnico, Allegato B del Decreto, per ulteriori dettagli e si utilizzi, per la ricognizione, il documento messo a disposizione dall'Amministrazione;
- individuare e nominare per iscritto gli Incaricati (personale strutturato e non dell'Ateneo) al trattamento dei dati, dettagliando i relativi compiti (ambito del trattamento consentito); inoltre:
 - fornire agli Incaricati una credenziale di autenticazione;
 - individuare per ciascun Incaricato o per classi omogenee di Incaricati i profili di autorizzazione;
 - individuare un Incaricato (Custode Password) che mantenga un apposito Registro con l'elenco dei codici identificativi e delle parole chiavi assegnati/revocati ed in generale utilizzati dagli Incaricati, allo scopo di assicurare la disponibilità dei dati e/o degli strumenti elettronici nei casi di assenza o impedimento degli Incaricati stessi per esclusive necessità di operatività e di sicurezza del sistema;
 - prescrivere, inoltre, a tale Incaricato l'adozione di adeguate misure di sicurezza al fine di garantire la segretezza delle informazioni contenute nel Registro e di informare tempestivamente l'Incaricato di ogni intervento eventualmente effettuato;

- prescrivere agli Incaricati di comunicare al Custode Password ogni variazione apportata sulle parole chiavi;
- fornire agli Incaricati specifiche istruzioni sulle modalità di trattamento dei dati nel rispetto della normativa vigente in tema di privacy e sicurezza: segretezza della componente riservata della credenziale per l'autenticazione, non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento, utilizzo e custodia diligenti dei dispositivi assegnati, utilizzo di password all'accensione del computer e di password di screen saver, salvataggio dei dati con frequenza almeno settimanale, custodia ed uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare trattamenti non consentiti, mantenere aggiornati gli antivirus...;
- con particolare riferimento agli aspetti informatici, anche tramite apposito incaricato:
 - introdurre idonei strumenti elettronici (firewall, intrusion detection, ...) per la protezione dei dati sensibili e giudiziari contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, e dare disposizioni per il corretto utilizzo;
 - introdurre idonei strumenti elettronici (antivirus) per la protezione dei server e di tutti gli apparati dal rischio di intrusione e dall'azione di programmi di cui all'art. 615- quinquies del codice penale, da aggiornare con scadenza almeno semestrale, e dare disposizioni per il corretto utilizzo;
 - impartire istruzioni per l'aggiornamento periodico, almeno con cadenza annuale, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti; in caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno con cadenza semestrale;
 - impartire istruzioni organizzative e tecniche agli Incaricati per il salvataggio dei dati con frequenza Almeno settimanale, per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati (ivi compreso il riutilizzo dei supporti e/o la relativa distruzione);
 - adottare idonee misure ed impartire istruzioni agli Incaricati, in caso di trattamenti di dati sensibili e/o giudiziari, per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi non superiori a sette giorni;
 - adottare misure ed impartire istruzioni agli Incaricati, nel caso di trattamento di dati personali idonei a rilevare lo stato di salute e la vita sessuale, per l'adozione di tecniche di cifratura o separazione di tali dati dagli altri dati personali dell'interessato; impartire, inoltre, istruzioni agli Incaricati, nel caso particolare di trattamento di dati relativi all'identità genetica, per l'utilizzo dei medesimi esclusivamente all'interno di locali protetti, o, in caso di trasporto dei dati all'esterno, per l'utilizzo di contenitori muniti di serratura o dispositivi equipollenti, o, in caso di trasferimento di dati in formato elettronico, per l'utilizzo di tecniche di cifratura;

- verificare periodicamente, almeno con cadenza annuale, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione e dell'ambito dei trattamenti consentiti;
 - informare il Titolare su ogni variazione inerente le banche dati cartacee e/o elettroniche di propria competenza;
 - collaborare con il Titolare per la predisposizione del documento programmatico sulla sicurezza.
10. Incaricati – E' compito degli Incaricati rispettare ed applicare ogni disposizione impartita dal Responsabile nel rispetto della normativa vigente in tema di privacy e sicurezza.
 11. Per tutto quanto non previsto nel presente regolamento si fa riferimento alle disposizioni del Decreto.
 12. Nell'ambito delle strutture e dei dipendenti dell'Università l'accesso ai dati personali ed il relativo trattamento è consentito esclusivamente al titolare e ai soggetti all'uopo nominati responsabili od incaricati.
 13. Tutto il personale, strutturato e non, dell'Ateneo, preposto stabilmente ed in modo documentato ad una struttura per la quale siano individuate per iscritto l'ambito del trattamento consentito agli addetti della struttura medesima, è automaticamente incaricato del trattamento dei dati necessario all'espletamento delle funzioni svolte nell'ambito della struttura ed è pertanto obbligato al rispetto delle prescrizioni previste dal presente regolamento.
 14. Il Rettore, avvalendosi di un apposito gruppo di lavoro nominato con proprio decreto, Coordinato dall'ufficio URP e rappresentativo del Titolare, assicura:
 - il massimo coordinamento nell'adempimento degli obblighi di tutela dei dati previsti dalla legge ed un più funzionale assolvimento dei compiti che il Decreto attribuisce al titolare e ai responsabili del trattamento dei dati
 - il controllo dell'uniforme applicazione delle misure minime di sicurezza di cui agli artt. 33-36 del Decreto e dei relativi Documenti Programmatici della Sicurezza, tenuto conto dell'articolazione delle strutture dell'Università e della pluralità delle unità amministrative esistenti
 - l'aggiornamento annuale della mappatura delle banche dati
 - il piano annuale degli interventi formativi atti a rendere edotti i responsabili e gli incaricati dei trattamenti dei rischi che incombono sui dati, delle misure di sicurezza atte a prevenire eventi dannosi e delle responsabilità che ne derivano.

Art.4 Misure di sicurezza

1. Il titolare e il responsabile dei dati custodiranno i dati adottando tutte le misure idonee ad evitare i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
2. In particolare, i titolari ed i responsabili della sicurezza dei dati, se designati, adottano, per la custodia dei dati personali raccolti negli archivi informatizzati e cartacei della struttura di appartenenza, le misure minime di sicurezza definite agli art. 33, 34,35 ed all'allegato B del Decreto.

3. I titolari del trattamento di dati personali con strumenti elettronici, entro il 28 febbraio di ciascun anno, devono redigere e/o aggiornare il Documento Programmatico della Sicurezza di cui allegato B del Decreto.

Art. 5 Notificazione delle banche di dati

Per consentire al titolare la notificazione delle banche di dati prevista dal Decreto, i responsabili che intraprendano o cessino il trattamento di dati, nell'ambito delle strutture universitarie, sono tenuti a comunicarlo al titolare mediante una comunicazione scritta che indichi:

- le finalità e modalità del trattamento ;
- la natura dei dati, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono ;
- l'ambito di comunicazione e diffusione dei dati ;
- gli eventuali trasferimenti di dati previsti verso Paesi non appartenenti all'Unione Europea o, qualora si tratti di dati sensibili o di dati relativi a provvedimenti di cui all'art.686 c.p.p., fuori dal territorio nazionale ;
- una descrizione delle misure di sicurezza adottate, che comunque non possono essere inferiori a quelle previste dagli artt. 34 e 35 del Decreto;
- l'eventuale connessione con altri trattamenti o banche dati;

Art. 6 Diritti dell'interessato

1. Le informazioni per iscritto di cui all'art. 13 del Decreto possono essere date anche mediante affissioni o deplianti o moduli e/o volantini ovvero annunci sulle pagine Web di Ateneo contenenti la clausola " i dati raccolti e/o detenuti dall'Università sono trattati in conformità al D.Lgs 30 giugno 2003, n.196".
2. Ogni struttura dell'Università dati provvederà ad assolvere agli obblighi di informativa imposti nei confronti dell'interessato ogni qualvolta si provveda alla raccolta di dati personali.
3. Il soggetto i cui dati sono contenuti in una banca di dati ha il diritto di ottenere, senza ritardo:
 - a. La conferma dell'esistenza o meno di trattamenti di dati 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 lettere a) e b) sono state portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi (art.7 D.Lgs 196/03);
4. L'interessato ha inoltre il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano ancorché pertinenti allo scopo della raccolta.

5. L'interessato può esercitare tali diritti con una richiesta scritta al responsabile della banca di dati.
6. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

PARTE II

MODALITA' DEL TRATTAMENTO E DELLE RICHIESTE DI ACCESSO

Art. 7 Requisiti dei dati personali e del loro trattamento

1. I dati personali oggetto di trattamento sono:
 - trattati in modo lecito e secondo correttezza;
 - raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
 - esatti e, se necessario, aggiornati;
 - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
 - 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 e successivamente trattati.
2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.
3. La comunicazione e la diffusione di dati personali detenuti dall'Università a soggetti pubblici, a privati o ad enti pubblici economici, oltre che il loro trattamento, sono ammessi nei casi previsti dagli articoli 18, 19, 20, 21, 22, 39, 76, 82, 84 e 135 del Decreto, salvo quanto previsto dai successivi articoli 10 e 11.
4. la tenuta e l'aggiornamento dell'inventario delle banche dati esistenti presso le strutture dell'Università è effettuato dal Titolare il quale dovrà altresì provvedere agli adempimenti di cui agli artt. 37-41 del Decreto.

Art. 8 Richieste di trattamento, diffusione e comunicazione dei dati personali

1. Ogni richiesta finalizzata ad ottenere il trattamento, la diffusione e la comunicazione dei dati personali anche contenuti in banche di dati deve essere scritta e motivata. In essa devono essere specificati gli estremi del richiedente e devono essere indicati i dati ai quali la domanda si riferisce e lo scopo per il quale sono richiesti. In particolare i soggetti privati devono presentare una richiesta scritta al responsabile, indicando:
 - il nome, la denominazione o la ragione sociale;
 - le finalità e le modalità di utilizzo dei dati richiesti;
 - l'eventuale ambito di comunicazione dei dati richiesti impegnandosi ad utilizzare i dati esclusivamente per le finalità e nell'ambito delle modalità indicate.

2. Agli uffici ed alle segreterie dell'Università è consentito comunque il rilascio a terzi di documenti contenenti dati personali dietro esibizione di atto di delega con firma autenticata dell'interessato, oppure atto di delega, senza firma autenticata, accompagnato dall'esibizione del documento di identità del delegante e del delegato anche in fotocopia.
3. Le richieste provenienti da enti pubblici finalizzate al trattamento, alla diffusione e alla comunicazione dei dati sono soddisfatte, purché non incompatibili con i fini istituzionali dell'Università degli Studi dell'Aquila, quando necessarie al perseguimento dei fini istituzionali dell'ente richiedente. Per la disciplina attinente ai soggetti pubblici si rinvia all'art. 19, c. 2 del Decreto.
4. L'Università, dopo avere valutato che il trattamento, 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.
5. Sul sito dell'Ateneo è disponibile la modulistica per l'accesso agli atti .

PARTE III

DIFFUSIONE E COMUNICAZIONE DEI DATI

Art. 9 Accesso a documenti amministrativi

1. Fatto salvo quanto previsto dal secondo comma (articolo 60 del Decreto), i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990 n. 241 e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in ottemperanza ad una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
2. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi 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.

Art. 10 Circolazione dei dati all'interno dell'Università

1. Le disposizioni contenute negli articoli che seguono s'intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno. L'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale l'Università provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne la conoscenza e la fruizione, anche presso le strutture didattiche e di ricerca.

2. Ogni richiesta d'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.
3. Chi richiede i dati, chi li riceve, chi li tratta e chi ne ha notizia è comunque vincolato al rispetto del segreto d'ufficio. La responsabilità penale, prevista dalla D.Lgs 196/2003 per l'uso non corretto dei dati personali conosciuti, resta a carico della singola Persona cui l'uso illegittimo si riferisca. In caso di condanna dell'Ente al risarcimento del danno, sia patrimoniale che non patrimoniale, esso potrà rivalersi sul responsabile.
4. Le richieste di dati personali provenienti da soggetti che ricoprono ruoli istituzionali si presumono effettuate all'esclusivo scopo di svolgere le attività inerenti alla funzione svolta. Laddove invece la richiesta fosse finalizzata ad un utilizzo ulteriore e/o diverso dei dati, sarà necessaria una richiesta scritta e motivata, ai sensi dell'art. 8 del presente regolamento.
5. Ai fini del trattamento dei dati sono equiparati alle strutture dell'Università gli organismi di controllo e di valutazione ed ogni altro organo, interno ed esterno a cui espresse disposizioni normative e/o regolamentari affidino tali compiti.

Art.11 Dati personali : personale docente e tecnico amministrativo

1. E' consentita la diffusione e la comunicazione a terzi dei dati personali secondo quanto previsto dagli artt. 24 e 137 del Decreto e, salvo opposizione dell'interessato ai sensi dell'art.7, comma 4, lettera a) dello stesso Decreto, è comunque permessa la diffusione e la comunicazione a terzi di dati relativi al personale, anche cessato, docente, ricercatore e tecnico-amministrativo dell'Università, nonché dei collaboratori professionali anche esterni, aventi a qualsiasi titolo un rapporto di lavoro con l'Ateneo e dei soggetti estranei all'Amministrazione, membri di organi collegiali e commissioni dell'Università, quando siano indicati esclusivamente:
 - nome, qualifica e dati ad essa relativi (quali il sommario dei corsi tenuti, le materie insegnate, l'elenco delle pubblicazioni effettuate, dati relativi ad attività di studio e di ricerca;
 - sede di servizio, ivi compreso il numero di telefono e di fax;
 - struttura di appartenenza dell'interessato ed organo collegiale di cui sia eventualmente membro.
2. In ogni caso non potranno essere diffusi o comunicati a terzi dati relativi allo stato matricolare, al rendimento ed all'efficienza, alla cessazione dallo status di docente o dipendente, alle azioni di responsabilità davanti alla Corte dei Conti, ai procedimenti penali, disciplinari e ad inchieste ispettive ad essi preliminari, salvi i casi di giustizia.
3. Il titolare di un corso può comunicare e diffondere anche mediante affissioni di elenchi gli esiti di esami, corsi e prove anche intermedie di vario tipo sostenute. La comunicazione via Web è consentita solo all'interessato.
4. Sono altresì permesse :
 - a) la diffusione e la comunicazione a terzi, anche a privati e per via telematica di dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e

tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli sensibili o giudiziari;

- b) la diffusione e comunicazione a terzi di dati statistici in forma anonima per scopi storici, statistici e scientifici.

Art.12 Dati personali: studenti e laureati

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale e nel mondo del lavoro, anche all'estero, dei giovani studenti e laureati, se non incompatibile con gli scopi istituzionali dell'Ateneo e previo consenso dell'interessato, si possono comunicare e diffondere, anche a privati e per via telematica, i dati:
 - relativi alle attività ed ai soggetti, compresi i diplomati universitari, di cui all'art. 100 del Decreto e solo per gli scopi ivi indicati;
 - relativi agli esiti scolastici, intermedi e finali, degli studenti, dei giovani laureati e laureandi, borsisti, specializzandi, dottorandi, allievi di corsi di formazione professionale o altri soggetti che comunque svolgano attività di studio e di ricerca presso l'Ateneo anche al fine di consentire l'invio ai soggetti sopra indicati, di inviti ad incontri, manifestazioni, riunioni, congressi, aventi ad oggetto tematiche connesse all'ambito universitario.

I predetti dati possono essere successivamente trattati per le sole finalità in base alle quali sono comunicati o diffusi
2. Resta fermo il diritto dell'interessato di opporsi per motivi legittimi ai sensi dell'art.7, comma 4, lettera a) del Decreto.

Art. 13 Disposizioni finali

Il presente regolamento entra in vigore dalla data della sottoscrizione del relativo decreto rettorale.