



UNIVERSITÀ DEGLI STUDI DI BRESCIA

Reg. XXXI N.473

IL RETTORE

VISTA la normativa vigente in materia di protezione dei dati personali (Privacy);

VISTO il D. Lgs. n. 33 del 14.03.2013, in particolare l'art. 4, relativo ai "Limiti alla Trasparenza" che introduce la possibilità per i dati personali, diversi dai dati sensibili e dai dati giudiziari di una loro diffusione attraverso siti istituzionali nonché il loro trattamento secondo modalità che ne consentano la indicazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo nel rispetto dei principi di legge sul trattamento dei dati personali;

RAVVISATA la necessità, ai fini dell'attuazione dei principi normativi, sopra riportati, di redigere un nuovo Regolamento in materia di protezione dati personali, identificando le tipologie dei dati trattati nell'ambito delle attività dell'Università degli Studi di Brescia, le finalità perseguite dal trattamento, le operazioni eseguite con gli stessi dati e le rispettive misure di sicurezza;

VISTA la delibera del Consiglio di Amministrazione n. 262/15610 del 28 ottobre 2013, con la quale è stato approvato il nuovo Regolamento di cui sopra, con l'allegato documento tecnico riservato, quest'ultimo sostitutivo del documento di protezione e sicurezza (DPS) con particolare riferimento alle nuove misure di sicurezza, organizzative e dei programmi informatici adottati dall'Università, il tutto, in sostituzione del precedente Regolamento, emanato con D.R. Reg. XXIV n. 220 del 23.12.2005;

RITENUTO, pertanto necessario emanare le nuove norme regolamentari, stabilendone l'entrata in vigore alla data del 1° novembre 2013

CIO' PREMESSO

DECRETA

1 - E' emanato il Regolamento di Ateneo in materia di protezione dei dati personali (Privacy) con l'Atto/documento tecnico, come da allegato che costituisce parte integrante e sostanziale del presente decreto.

2 - Il predetto documento tecnico, in considerazione dei suoi contenuti e finalità è da ritenersi "atto riservato" e come tale, viene, pertanto, conservato presso l'U.A.S. Affari Legali di questa Università.

3 - Il Regolamento entra in vigore a decorrere dal 1° novembre 2013

Brescia, 31/10/2013

Il Rettore
(Prof. Sergio Pecorelli)

REGOLAMENTO IN MATERIA DI PROTEZIONE DATI (PRIVACY)

Art. 1) DEFINIZIONI

Per “**Sistema Informativo**” s’intende l’insieme delle risorse umane, delle regole organizzative, delle risorse informatiche, dei locali e della documentazione che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti alle attività dell’Università degli Studi di Brescia (d’ora in avanti denominata Ateneo). Tutti i dati contenuti nel predetto sistema sono protetti secondo la normativa vigente.

Per “**Dato Comune**” s’intendono tutte le informazioni relative a persone fisiche o giuridiche.

Per “**Dato Identificativo**” s’intendono i dati personali che permettono l’identificazione diretta dell’interessato.

Per “**Dato Sensibile**” s’intende ogni informazione relativa:

- all’origine razziale ed etnica;
- alle convinzioni religiose e filosofiche;
- alle opinioni politiche, all’adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, politico, sindacale e filosofico;
- allo stato di salute. Sono qui compresi i dati sanitari per i quali quelli genetici possono essere oggetto di trattamento nei limiti dell’autorizzazione del Garante (n. 8/2012). Tali dati possono essere generalmente richiesti per specifici obblighi o esecuzione di specifici compiti previsti dalla normativa nazionale e comunitaria o da regolamenti, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali e degli infortuni e di diagnosi;
- alla vita/orientamento sessuale.

Per “**Dati Giudiziari**” s’intendono quei dati personali idonei a rilevare provvedimenti in materia di casellario giudiziale e possono essere così indicati:

- provvedimenti di condanna definitivi, anche pronunciati da autorità giudiziarie straniere se riconosciuti ai sensi degli articoli 730 e ss. c.p.p., salvo quelli concernenti contravvenzioni per le quali la legge ammette la definizione in via amministrativa, o l’oblazione limitatamente alle ipotesi di cui all’articolo 162 c.p., sempre che per quelli esclusi non sia stata concessa la sospensione condizionale della pena;
- provvedimenti giudiziari definitivi concernenti le pene, compresa la sospensione condizionale e la non menzione, le misure di sicurezza personali e patrimoniali, gli effetti penali della condanna, l’amnistia, l’indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a delinquere;
- provvedimenti giudiziari concernenti le pene accessorie;
- provvedimenti giudiziari concernenti le misure alternative alla detenzione e quelli concernenti la liberazione condizionale;
- provvedimenti giudiziari definitivi che hanno prosciolto l’imputato o dichiarato non luogo a procedere per difetto d’imputabilità, o disposto una misura di sicurezza;
- provvedimenti giudiziari concernenti la riabilitazione;
- provvedimenti giudiziari relativi all’espulsione a titolo di sanzione sostitutiva o alternativa alla detenzione;
- provvedimenti di correzione e ogni altro provvedimento definito a norma di legge.

Per “**Dati Particolari**” si intendono quei dati appartenenti alla categoria intermedia tra i dati sensibili e quelli comuni. Pertanto, per la loro natura vengono trattati nel rispetto di specifiche modalità e accorgimenti prescritti a garanzia dell’interessato.

Per “**Trattamento**” si intende qualunque operazione o complesso di operazioni effettuate, anche senza l’ausilio di strumenti elettronici, concernenti:

- la raccolta, la registrazione, la modificazione delle caratteristiche originarie,
- le integrazioni, la selezione relativa alla classificazione e categorizzazione,
- il raffronto secondo accertamento dell’identità,
- le statistiche e ricerche varie,
- la consultazione e/o l’utilizzo e l’interconnessione con altre fonti informative,
- il blocco, la sospensione temporanea,
- la comunicazione/diffusione a uno o più soggetti individuabili,
- la custodia, la cancellazione e la distruzione dei dati stessi.

Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, esso 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.

L'Ateneo, sulla base della propria organizzazione e delle relative strutture di riferimento, individua i compiti e le relative responsabilità in relazione ai trattamenti effettuati. Ciò coerentemente con quanto indicato dagli artt. 28, 29 e 30 del D. Lgs. n. 193/2003.

L'Ateneo si riserva, comunque, di nominare ulteriori soggetti responsabili del trattamento, a seguito di mutamenti organizzativi e qualora si rendesse opportuno e necessario per lo svolgimento delle proprie attività istituzionali, comunicare e/o delegare a soggetti terzi esterni all'Ateneo il trattamento di alcuni dati.

Per **Soggetti del trattamento dei dati** si intendono:

- **TITOLARE:** è il Rettore dell'Ateneo, in quanto rappresentante legale, domiciliato per la carica presso la sede legale, cui competono, anche unitamente ad eventuale suo delegato, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza informatica. Il titolare è tenuto ad adottare tecnologie e soluzioni applicative atte a ridurre al minimo qualsiasi tipo di rischio; a organizzarsi, anche, sotto il profilo tecnologico, al fine di consentire un'adeguata attuazione della normativa.
- **RESPONSABILE:** è il responsabile della struttura –Dipartimento e Aree/Servizi- a cui compete il trattamento dei dati. Deve essere designato dal Titolare. Il Responsabile della struttura incarica, con proprio provvedimento formale, coloro che devono effettuare operativamente il trattamento dei dati personali, verificando che abbiano la preparazione adeguata e curando gli aggiornamenti periodici. Di questi ultimi va data tempestiva comunicazione al Titolare del trattamento.
- **INCARICATI:** sono persone fisiche autorizzate a compiere operazioni di trattamento dal Responsabile, operano sotto la diretta autorità del Titolare o del responsabile, attenendosi alle istruzioni/direttive impartite. La designazione è effettuata per iscritto e individua, precisamente, l'ambito del trattamento consentito. Gli incaricati si differenziano tra Incaricati al trattamento e Amministratori di sistema. I primi operano direttamente con i dati ai fini di realizzare in modo diretto i processi amministrativi e quindi utilizzano sistemi applicativi gestionali o sistemi di elaborazione personale dei dati. I secondi non operano direttamente con i dati ma amministrano i sistemi per l'elaborazione dei dati e, in quanto tali, possono accedere ai dati stessi.

Art. 2) **MODALITA' DI RACCOLTA E REQUISITI DEI DATI PERSONALI**

I Responsabili dei dati devono verificare che i dati personali, oggetto di trattamento, siano:

- 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 non incompatibili con tali scopi;
- esatti e aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2.1 MISURE MINIME DI SICUREZZA

Le misure minime di sicurezza sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

- senza l'ausilio di strumenti elettronici;
- con strumenti elettronici.

Le procedure di sicurezza per la gestione dei dati con strumenti elettronici sono dettagliate nel documento allegato e parte integrante del presente regolamento al n. 1. "Documento tecnico sulla sicurezza informatica per la protezione dei dati personali".

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

2.2 CUSTODIA

I documenti contenenti dati personali devono essere custoditi in modo tale da non essere accessibili a persone non incaricate del trattamento. In particolare: a) i documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana, devono essere riposti a fine giornata; b) i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro; c) i documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Incaricati in modo tale che non vi accedano

persone prive di autorizzazione. L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassette chiusi a chiave.

2.3 COMUNICAZIONE

L'utilizzo dei dati personali deve avvenire in base al principio del "need to know" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni o ruolo lavorativi. I dati non devono essere comunicati all'esterno dell'Ateneo e comunque a soggetti terzi se non previa autorizzazione.

2.4 DISTRUZIONE

Qualora sia necessario distruggere i documenti contenenti dati, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo tale da non essere più riconoscibili. I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non fosse possibile, essi devono essere distrutti.

Art. 3) DIRITTI DELL'INTERESSATO

L'interessato ha diritto:

- di conoscere l'esistenza o meno di dati personali che lo riguardano e di conoscerne l'origine;
- di essere informato dal titolare circa le finalità e modalità del trattamento;
- di ottenere dal titolare l'aggiornamento, la rettificazione ovvero l'integrazione dei dati trattati;
- di conoscere gli estremi identificativi del titolare e del responsabile del trattamento;
- di opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati che lo riguardano;
- di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

Il riscontro alla richiesta formulata dall'interessato è fornito dal titolare o dal responsabile o dal delegato di quest'ultimo, entro 15 giorni dal suo ricevimento. Entro tale termine, se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di 30 giorni dal ricevimento della richiesta stessa.

L'interessato, al fine di tutelare i propri diritti, può agire direttamente nei confronti del titolare, del responsabile, chiedendo il ripristino dei diritti violati.

Art. 4) INFORMATIVA

Ogni responsabile assolve agli obblighi di informativa previsti dalla Legge e dal presente Regolamento, tutte le volte che si provveda alla raccolta di dati personali, avvalendosi della modulistica/clausole ove disponibile.

Art. 5) NOTIFICAZIONE

I Responsabili devono notificare al Titolare le finalità e le modalità di gestione del trattamento. In particolare, la suddetta comunicazione deve contenere:

- la natura dei dati, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono;
- gli eventuali trasferimenti di dati verso Paesi non appartenenti all'Unione Europea o, qualora si tratti di dati sensibili o giudiziari, fuori del territorio nazionale;
- l'ambito di comunicazione e diffusione dei dati;
- una descrizione generale che permetta di valutare l'adeguatezza delle misure tecniche ed organizzative adottate per la sicurezza dei dati;
- l'eventuale connessione con altri trattamenti o banche dati.

Quanto sopra dovrà essere notificato anche nel caso in cui i responsabili intendano cessare dalla designazione al trattamento dei dati.

Art.6) RICHIESTE DI TRATTAMENTO, DIFFUSIONE E COMUNICAZIONE DEI DATI PERSONALI

Ogni richiesta rivolta all'Ateneo, finalizzata ad ottenere il trattamento, la diffusione e la comunicazione di dati personali dev'essere scritta e motivata. In essa devono essere specificati gli estremi del richiedente e devono essere indicati con esattezza i dati ai quali la domanda si riferisce e lo scopo per il quale gli stessi sono richiesti. Le richieste provenienti da Enti pubblici saranno soddisfatte quando sono necessarie al perseguimento dei fini istituzionali dell'ente richiedente o quando il conferimento dei dati sia previsto da esplicite disposizioni di legge.

Art. 7) AFFIDAMENTO A TERZI DI DATI PERSONALI

L'Ateneo ha la facoltà di stipulare specifiche convenzioni che attribuiscono a società o consorzi interuniversitari la gestione dei dati personali, nell'ambito dei propri fini istituzionali e nel rispetto della normativa vigente e del presente Regolamento.

Per maggior precisazione in merito al contenuto delle modalità di gestione dei dati, oggetto delle convenzioni di cui sopra, si rinvia al Documento Tecnico, allegato n. 1.

Art. 8) PROCEDURE DI RIPRISTINO IN CASO DI INTERRUZIONE DEL SERVIZIO

Il ripristino del servizio di trattamento informatico dei dati viene effettuato direttamente dal personale interno all'Ateneo o, nel caso di servizi affidati a ditte esterne, da personale specializzato su specifica richiesta e controllo dei Responsabili di struttura. Tali procedure sono finalizzate a fornire il massimo grado di tutela delle risorse dell'Ateneo.

Art. 9) DISPOSIZIONI FINALI

L'individuazione degli incaricati al trattamento dati è soggetta a periodico aggiornamento, così come i criteri per l'individuazione dei rispettivi responsabili.

In considerazione dei contenuti e delle finalità, circa le misure di sicurezza e di protezione dei dati, il Documento Tecnico, allegato n. 1 è da considerarsi Atto Riservato. Esso viene, pertanto, conservato agli atti dell'Amministrazione e sarà esibito, su richiesta, all'Autorità giudiziaria e/o al Garante per la protezione dei dati personali. Qualsiasi altra richiesta di accesso da parte di terzi, purché motivata, potrà essere accordata, previa autorizzazione da parte del Titolare e, comunque, limitatamente alla parte di specifico interesse del richiedente.

Sono fatti salvi i diritti di accesso previsti dalla legge n. 241/1990 e successive modificazioni o integrazioni e dal regolamento attuativo.

In merito alle forme di tutela, si rimanda al testo dell'articolo 10 del D.Lgs n. 150 del 01.09.2011.

Il presente Regolamento, adottato dai competenti Organi Accademici, è emanato con provvedimento rettorale ed entra in vigore il giorno della sua emanazione.

Verrà data allo stesso massima diffusione, pubblicato sul sito dell'Ateneo, secondo le vigenti regole di pubblicità legale e nelle forme di comunicazione ritenute più idonee ed efficaci.

Brescia,
