UNIVERSITÀ
di VERONA

REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI

(emanato con Decreto Rettorale rep. n. 1555 del 26 settembre 2017 – entrato in vigore il 13 ottobre 2017)

UNIVERSITÀ di VERONA

INDICE

UNIVERSITÀ di VERONA

TITOLO I – LE PREMESSE

Articolo 1 – Oggetto, ambito e scopo

1. Il presente regolamento contiene disposizioni attuative del d.lgs. n. 196/2003 e ss.mm. "*Codice in materia di protezione dei dati personali*" (di seguito indicato come Codice Privacy o, più semplicemente, Codice) nell'ambito delle strutture dell'Università degli Studi di Verona.
2. Scopo del Regolamento è garantire che le procedure per il trattamento dei dati personali da parte dell'Ateneo avvengano nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza ed all'identità personale degli utenti, sia interni che esterni e di tutti coloro che hanno rapporti con l'Ateneo stesso.
3. Ai fini del presente Regolamento vengono assunte le definizioni di cui al Codice Privacy tenuto conto, per quanto di competenza, del Regolamento UE 2016/679 del 27 aprile 2016.

TITOLO II – I SOGGETTI

Articolo 2 – Soggetti

1. Il trattamento dei dati personali, in conformità a quanto previsto dal Codice Privacy, è ammesso solo da parte dei soggetti di seguito indicati:
Titolare;
Responsabili del trattamento dei dati;
Incaricati.
2. Il titolare effettua tutte le nomine e le lettere di incarico relative alle figure coinvolte, laddove sia necessario, ricorrendo anche all'associazione per classi omogenee di incarico secondo quanto previsto dall'art. 30 del Codice.

Articolo 3 – Titolare del trattamento

1. Il Titolare del trattamento dei dati è l'Ateneo rappresentato dal Rettore.
2. Al Titolare del trattamento competono le decisioni in ordine alla finalità e alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
3. Il Titolare del trattamento deve assicurare e garantire che vengano adottate le misure di sicurezza ai sensi del Codice.
4. È onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati.
5. Il Titolare del trattamento affida ai Responsabili del trattamento dei dati il compito di applicare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite a mezzo del Documento sulla Privacy e la Sicurezza informatica di cui all'art. 16 del presente regolamento.
6. Informa i Responsabili del trattamento dei dati delle responsabilità loro affidate e delle norme riguardanti in specie la sicurezza del trattamento dei dati in vigore, in particolare di quanto stabilito dal Codice nonché di eventuali aggiornamenti.
7. Il Titolare del trattamento dei dati nomina la Commissione Privacy che ha funzione consultiva e di proposta nell'adempiere agli obblighi previsti dalla normativa nazionale in materia di riservatezza dei dati personali nonché dal presente regolamento.

Articolo 4 – Responsabili del trattamento

4.1 La nomina

1. I Responsabili sono individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
2. Presso l'Ateneo l'incarico di Responsabile del trattamento dei dati coincide di norma con la titolarità di un incarico di responsabilità di Centro di Responsabilità, di Dirigente oppure con la posizione di Direttore di Dipartimento.

3. L'assunzione del ruolo di Responsabile richiede specifica nota con precisazione, laddove necessario, delle funzioni da svolgere e dei relativi compiti.
4. L'individuazione del Responsabile del trattamento:
- è pro tempore,
- decade per revoca o dimissioni dello stesso
- è revocabile in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

4.2 Le funzioni
1. Il Responsabile del trattamento dei dati, nell'ambito della propria struttura di riferimento, ha il compito di:
- individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento;
- verificare che il trattamento dei dati sia effettuato secondo le norme vigenti;
- istruire chiaramente gli incaricati circa le modalità di trattamento dei dati, con o senza l'ausilio di strumenti elettronici;
- verificare, almeno con cadenza annuale, l'integrità dei profili di autorizzazione degli incaricati del trattamento dei dati, con o senza l'ausilio di strumenti elettronici;
- garantire che tutte le misure di sicurezza riguardanti i dati personali afferenti alla struttura siano applicate all'interno ed eventualmente al di fuori della stessa, qualora siano trasferite o delegate a soggetti terzi, quali Responsabili del trattamento, tutte o parte delle attività di trattamento, con o senza l'ausilio di strumenti elettronici;
- informare il Titolare del trattamento della eventualità che si siano rilevati dei rischi per la sicurezza dei dati al cui trattamento è preposto e notificare allo stesso e a chi di competenza ogni mutamento delle misure di sicurezza adottate.

4.3 La responsabilità esterna
1. Al fine di dar seguito alla disciplina dettata dal Codice Privacy con riferimento alla comunicazione dei dati personali a terzi (solo se prevista da una norma di legge o di regolamento ovvero per espresso consenso dell'interessato), nei contratti, rapporti o convenzioni con cui l'Ateneo affida a terzi attività che comportano il trattamento di dati personali (es. ipotesi di esternalizzazione di servizi) non vi è alcuna autonomia del terzo per quanto riguarda il trattamento, che resta prerogativa esclusiva dell'Ateneo. Quest'ultimo nomina il terzo contraente come Responsabile esterno dei trattamenti dei dati personali effettuati in forza del rapporto contrattuale o convenzionale.
2. Il Responsabile esterno, entrato in questo modo a far parte del "*sistema privacy*" dell'Ateneo, che rimane Titolare del trattamento, è legittimato ad utilizzare, negli stretti limiti in cui siano indispensabili per l'espletamento dell'incarico affidato, dati personali in possesso dell' Ateneo.

Articolo 5 – Incaricati del trattamento

5.1 – La nomina
1. Con riferimento al personale dipendente, la designazione ad Incaricato del trattamento dati viene effettuata per iscritto dal Titolare o dal Responsabile, oppure si considera come designazione ad incaricato la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Tra gli incaricati vanno considerati anche i Responsabili scientifici di un progetto di ricerca ed i componenti del gruppo di ricerca.
2. La nomina ad "incaricato" costituisce presupposto di liceità dei trattamenti dati.
3 Nei casi non previsti dal comma 1, la nomina di ciascun Incaricato del trattamento deve essere effettuata con una lettera di incarico in cui sono specificati i compiti che gli sono affidati.
4. La nomina degli Incaricati è a tempo indeterminato, e decade per revoca, per sue dimissioni dall'Ateneo, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

5.2 – Le funzioni
1. Gli incaricati sono le persone fisiche autorizzate dal titolare o dal responsabile a compiere, sotto la loro autorità, operazioni di trattamento, cioè coloro che materialmente effettuano, attenendosi alle istruzioni impartite

dal titolare e dal responsabile, le operazioni di trattamento di dati.
2. Agli Incaricati del trattamento, per ottemperare agli obblighi di sicurezza dei dati, il Titolare o il Responsabile indica e rende disponibili tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina del trattamento e gli stessi sono tenuti ad informarsi ed aggiornarsi, anche mediante la partecipazione agli incontri e seminari formativi che vengano in materia organizzati dal Titolare.

Articolo 6 – Amministratori di sistema

6.1 – La definizione
1. L'Amministratore di Sistema (AdS) è la figura dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning), le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
2. L'AdS assume vari ruoli:
- amministratore delle basi di dati (database administrator), responsabile dell'integrità dei dati stessi, dell'efficienza e delle prestazioni del sistema-database;
- amministratore della rete (network administrator) che gestisce l'infrastruttura di rete (apparati come hub, switch e router) ed effettua le diagnosi dei problemi che i vari personal computer o server hanno con essa;
- amministratore della sicurezza (security administrator), compresa la gestione dei dispositivi tipo firewall e l'adozione di misure di sicurezza generale;
- amministratore web (web administrator), che si preoccupa della gestione dei servizi web, ovvero servizi che permettono ad utenti interni o esterni di accedere ai siti web
3. Non rientrano in questa categoria quei soggetti che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software per scopi di manutenzione a seguito di guasti o malfunzionamenti.
4. Le principali funzioni dell'AdS comportano un'effettiva capacità di azione sulle informazioni, contenute all'interno del sistema informatico, tanto da poter costituire a tutti gli effetti un trattamento di dati personali, anche quando le informazioni non sono consultabili "in chiaro".

6.2 - La nomina
1. Il Titolare del trattamento dei dati o i Responsabili del trattamento preposti a strutture che lo necessitano possono nominare uno o più AdS, specificando gli elaboratori, le reti, gli applicativi complessi o le banche dati che sono chiamati a sovrintendere, informandoli delle responsabilità che sono loro affidate in relazione a quanto disposto dalle normative in vigore.
2. Per procedere all'attribuzione delle funzioni di AdS, devono essere valutate preventivamente le caratteristiche personali e professionali del soggetto, che deve possedere requisiti di esperienza, capacità e affidabilità, nonché dare garanzia del rispetto, oltre che della conoscenza, delle disposizioni in materia di trattamento dei dati personali, sicurezza compresa. Gli stessi sono tenuti ad informarsi ed aggiornarsi al riguardo, anche mediante la partecipazione agli incontri e seminari formativi che vengano in materia organizzati dal Titolare.
3. La designazione individuale dell'AdS deve seguire un preciso profilo di autorizzazione, mediante affidamento di specifici ambiti di operatività e evitando ogni accesso a dati eccedenti rispetto le necessità della sua azione.
4. La lettera di incarico deve contenere:
- l'attestazione che l'incaricato ha le caratteristiche richieste;
- l'elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato;
- l'indicazione delle verifiche almeno annuali che il titolare o il responsabile delegato dovranno svolgere sulle attività svolte dell'amministratore di sistema;
- l'indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed eventualmente a terzi nei modi richiesti dalla normativa vigente.
5. La lettera di incarico deve essere controfirmata dall'interessato per presa visione e accettazione.
6. Gli estremi identificativi delle persone fisiche, che ricoprono il ruolo di AdS, dovranno essere contenuti in un elenco in cui siano riportate le funzioni loro attribuite.

6.3 – La verifica dell'attività
1. L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Articolo 7 – Commissione Privacy
1. La Commissione Privacy, nominata dal Titolare del trattamento e composta da esperti tecnici e giuridici in materia, svolge i seguenti compiti:
- garantisce il supporto giuridico, tecnico e di consulenza al Titolare per quanto riguarda gli adempimenti derivanti dalla normativa in materia di protezione dei dati personali;
- collabora alla compilazione periodica del "Documento di valutazione della privacy" con i Responsabili del trattamento;
- suggerisce progetti formativi, incontri e seminari in materia di privacy e sicurezza informatica rivolti a tutti i soggetti autorizzati al trattamento dei dati personali;
- promuove l'osservanza del presente regolamento;
- collabora con il Titolare e i Responsabili del trattamento all'elaborazione periodica di una Policy di Ateneo sulla Sicurezza Informatica, proponendo l'adeguamento dei percorsi e delle procedure alle disposizioni normative e regolamentari vigenti nonché ai provvedimenti del Garante in materia di riservatezza dei dati;
- fornisce, su richiesta, la necessaria consulenza in ordine alle problematiche in materia di riservatezza, collaborando con i Responsabili del trattamento;

TITOLO III – REGOLE SUL TRATTAMENTO DEI DATI

CAPO I – MODALITA' PER IL TRATTAMENTO DEI DATI PERSONALI

Articolo 8 – Modalità di raccolta e requisiti dei dati personali
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 non incompatibili 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 sistemi informativi sono configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali ed identificativi ed in modo da evitare il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o modalità di identificazione dell'interessato solo in caso di necessità.

Articolo 9 - Diritto all'oblio
1. Il diritto dell'interessato di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano, per i motivi e secondo le modalità indicati nei paragrafi 1 e 2 dell'art. 17 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, può essere esercitato e fatto valere nei confronti dell'Ateneo tenendo conto dei motivi di esclusione previsti dal paragrafo 3 del citato art. 17, ed in specie della natura di ente pubblico dell'Ateneo, delle funzioni e dei servizi pubblici che svolge, dei suoi regolamenti e delle finalità istituzionali cui è funzionale lo stesso trattamento dei dati personali, che di regola non avviene su base meramente consensuale.

Articolo 10 - Trattamento di dati sensibili e giudiziari
1. Nelle ipotesi in cui la legge autorizzi il trattamento di dati sensibili per il perseguimento di finalità di rilevante interesse pubblico, senza specificare i tipi di dati sensibili e le operazioni eseguibili, il trattamento è consentito alle condizioni e nei limiti previsti dal vigente Regolamento per il trattamento dei dati sensibili e giudiziari adottato dall'Ateneo e conforme allo schema tipo per il sistema universitario approvato dal Garante per la

protezione dei dati personali.

Articolo 11 - Videosorveglianza
1. L'Ateneo ha adottato un proprio Regolamento in materia di videosorveglianza presso le sedi dell'Università degli Studi di Verona che disciplina il trattamento dei dati personali realizzato mediante l'uso di sistemi di videosorveglianza.

Articolo 12 – Informativa all'interessato
1. L'informativa è l'elemento propedeutico al trattamento dei dati personali in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere.
2. L'informativa è sempre dovuta a prescindere dall'obbligo di acquisizione del consenso. L 'Ateneo in qualità di soggetto pubblico non è tenuto a chiedere il consenso all'interessato (art. 18 co. 4 Codice), salvi i casi prescritti da specifiche disposizioni.
3. Ciascun Responsabile fornisce agli interessati, ogniqualvolta provveda alla raccolta di loro dati personali, idonea informativa nella quale siano specificate:
- le finalità e le modalità del trattamento cui sono destinati i dati richiesti;
- la natura obbligatoria o facoltativa del conferimento di dati richiesti e le conseguenze di un eventuale rifiuto a fornirli;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
- i diritti spettanti all'interessato ai sensi dell'art. 7 del Codice;
- gli estremi identificativi del titolare e dei responsabili.
3. L'informativa può essere resa anche oralmente, per il tramite degli incaricati, ovvero inserita in moduli e formulari, affissa nei locali aperti al pubblico o ancora inclusa in pagine Web.

CAPO II – MISURE DI SICUREZZA

Articolo 13 – Adozione delle misure di sicurezza
1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
2. Il Titolare definisce le misure minime di sicurezza ai fini della privacy, oltre che con il presente Regolamento, attraverso il proprio sito internet alla sezione "*Privacy*". A tali documenti e ad altri ad uso interno, in particolare il Documento sulla Privacy e la Sicurezza Informatica di cui all'art. 16, viene data ampia diffusione tra il personale dipendente con la loro pubblicazione nell'Intranet, oltre che mediante specifici incontri e corsi formativi ove opportuno.
3. Agli incaricati è richiesto di custodire e trattare i dati applicando le misure idonee ad evitare rischi di distruzione o perdita, anche accidentale, e di accesso non autorizzato, riassunte nelle indicazioni sulla sicurezza predisposte dall'Ateneo oppure riportate nell'informativa allegata alla lettera di nomina, laddove sia necessaria, salvi i successivi aggiornamenti.
4. Tutti i Responsabili del trattamento dei dati sono tenuti ad adottare le misure di sicurezza, ulteriori rispetto a quelle minime prescritte dalla normativa nazionale a tutela della riservatezza dei dati personali, che si rendano necessarie in relazione a specifiche esigenze della struttura gestita, tenuto conto del livello di esposizione a rischio cui sono soggette le attività di trattamento dati affidate, della peculiarità e delicatezza dei trattamenti effettuati, nonché dello sviluppo tecnologico.
5. Ai Responsabili del trattamento dei dati è richiesto di vigilare sul rispetto, da parte degli incaricati, delle misure di sicurezza.

Articolo 14 – Copie di sicurezza delle banche dati
1. Il Responsabile del trattamento individua l'incaricato per le copie di sicurezza delle banche dati, di norma coincidente con l'Amministratore di Sistema, a cui è conferito il compito di effettuare e custodire le copie di

salvataggio dei dati archiviati nei sistemi di elaborazione dei dati.
2. È compito dell'incaricato delle copie di sicurezza delle banche dati:
- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti;
- assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro ad accesso controllato;
- provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato;
- segnalare tempestivamente al Responsabile di riferimento ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Articolo 15 - Sicurezza degli archivi cartacei
1. Gli atti e i documenti cartacei contenenti dati personali, sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
2. L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato e pertanto le persone ammesse, a qualunque titolo, devono essere identificate e registrate.
3. Se gli archivi cartacei non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

Articolo 16 - Documento sulla Privacy e la Sicurezza Informatica
1. Ai fini della valutazione della corretta adozione e del periodico aggiornamento delle misure minime di sicurezza, il Titolare predispone periodicamente, sentita la Commissione Privacy, il "Documento sulla Privacy e la Sicurezza Informatica" (DPSI), sulla base dell'analisi dei rischi che incombono sui trattamenti di dati, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento, delle misure in essere e da adottare, nonché dei criteri e delle modalità di ripristino della disponibilità dei dati.
2. Il DPSI, da ritenersi documento interno, deve contenere:
- la rilevazione aggiornata dei trattamenti, dei rischi e delle misure da adottare;
- la programmazione aziendale per l'attività di formazione degli incaricati e dei Responsabili del trattamento al fine di un utilizzo consapevole delle informazioni gestite;
- la raccolta delle informazioni in merito alla responsabilità dei dati personali affidata all'esterno (es. outsourcing);
3. Per la redazione del DPSI ed il relativo aggiornamento il Titolare si può avvalere oltre che della collaborazione della Commissione Privacy d'Ateneo, delle competenze tecniche e giuridiche di esperti in materia e di pareri dei Responsabili del trattamento.

Articolo 17 – Attività formativa
1. L'Ateneo riconosce l'importanza della formazione del personale sulle tematiche che riguardano la sicurezza e la privacy, come elemento significativo di riduzione dei rischi e si impegna a promuovere per tutti gli addetti adeguati momenti formativi e di aggiornamento.
2. Particolare attenzione deve essere prestata nella predisposizione di attività formative rivolte ai nuovi addetti, al momento dell'ingresso in servizio.
3. Gli interventi formativi devono essere anche programmati in modo tale da avere luogo al verificarsi delle seguenti circostanze:
- al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione dell'introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali
- in occasione di significative modifiche della disciplina giuridica sia esterna che interna.
4. Ai Responsabili del trattamento dei dati è affidato il compito di verificare ogni anno le necessità di formazione e aggiornamento del personale incaricato del trattamento dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.

Articolo 18 – Tutela della riservatezza nella redazione degli atti amministrativi
1. I responsabili delle strutture organizzative che propongono una delibera o che adottano una determinazione dirigenziale verificano, alla luce dei principi di pertinenza e non eccedenza sanciti dal Codice, che l'inclusione nel testo di dati personali sia realmente necessaria per perseguire le finalità proprie del provvedimento. Devono essere privilegiate modalità di redazione che prevedano l'utilizzo di dati anonimi o non direttamente identificativi, quali codici o altri riferimenti, se lo scopo cui l'atto è preordinato è ugualmente raggiungibile.
2. Laddove gli allegati alle delibere o alle determinazioni dirigenziali contengano dati sensibili tutelati dalla normativa sulla privacy, che non è possibile rendere anonimi, nel provvedimento dovrà essere evidenziato che l'allegato non viene pubblicato all'Albo, rimanendo depositato agli atti presso la struttura organizzativa, per esigenze di tutela della riservatezza dei destinatari del provvedimento o di terzi. Sull'allegato dovrà essere apposta la dizione "Riservato ai sensi delle vigenti norme sulla privacy".

TITOLO IV – NORME FINALI

Articolo 19 - Norme di rinvio
1. Le norme del presente Regolamento trovano applicazione in conformità e ad integrazione delle disposizioni del Codice Privacy, dei Provvedimenti del Garante, del Regolamento U.E. 2016/676 nonché dei regolamenti di Ateneo relativi rispettivamente al trattamento dei dati sensibili e giudiziari, all'utilizzo della posta elettronica e internet ed in materia di videosorveglianza.

Articolo 20 - Entrata in vigore
1. Il presente Regolamento è approvato dal Senato Accademico, previo parere favorevole del Consiglio di Amministrazione ed è emanato con Decreto del Rettore.
2. Se non diversamente stabilito nel Decreto di emanazione, entra in vigore il quindicesimo giorno successivo alla data di pubblicazione all'albo ufficiale dell'Università ed è reso disponibile sul sito web istituzionale.
3. Le modifiche al presente Regolamento seguono le medesime modalità di approvazione ed entrata in vigore previste al comma 1 e 2 del presente articolo.