UNIVERSITÀ DEGLI STUDI DI MILANO

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DELL'UNIVERSITÀ DEGLI STUDI DI MILANO

INDICE

PARTE GENERALE

Art. 1
AMBITO DI APPLICAZIONE

1. Il presente Regolamento, adottato in attuazione del Regolamento UE 27 aprile 2016 n. 679 (di seguito «*Regolamento UE*») e del D. Lgs. n. 196/2003 come novellato dal D. Lgs. n. 101/2018 (di seguito «*Codice in materia di protezione dei dati personali*» o «*Codice*»), disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali all'interno dell'Università degli Studi di Milano.

2. L'Università provvede al trattamento dei dati personali per lo svolgimento dei propri fini istituzionali, nei limiti stabiliti dallo Statuto, dalle leggi e dai regolamenti e in ogni caso nel rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato, con riferimento particolare alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Art. 2

DEFINIZIONI

1. Ai fini del presente Regolamento si intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, a titolo esemplificativo mediante il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «categorie particolari di dati»: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; i dati genetici; i dati biometrici; i dati relativi alla salute, alla vita sessuale e all'orientamento sessuale;

3) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

4) «dati biometrici»: i dati personali ottenuti da un trattamento specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

5) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

6) «interessato»: la persona fisica cui si riferiscono i dati personali;

7) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

8) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo dei dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

9) «processo decisionale automatizzato»: decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti nella sfera giuridica dell'interessato o che incide in modo analogo significativamente sullo stesso;

10) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;

11) "informazioni anonime": ai sensi del considerando 26 del GDPR informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato;

12) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

13) «Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

14) «Responsabile della protezione dei dati personali» o «DPO» (Data Protection Officer): figura specializzata nel supporto al Titolare, che svolge funzioni di raccordo con il Garante e di tutela degli interessati;

15) «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

16) «Designato»: figura apicale della struttura d'Ateneo che ha il compito di vigilare, monitorare e garantire il rispetto delle norme vigenti in materia di protezione dei dati personali, individuato ai sensi dell'Allegato al presente Regolamento;

17) «Referente»: soggetto appositamente individuato tra gli Autorizzati al trattamento operanti nella struttura del Designato e da questi assegnato alla gestione delle tematiche privacy;

18) «Autorizzati al trattamento»: le persone fisiche formalmente autorizzate e istruite a trattare i dati personali sotto la diretta autorità del Titolare;

19) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali;

20) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo diversi dall'interessato, dal Titolare del trattamento, dal Responsabile del trattamento e dalle persone Autorizzate al trattamento;

21) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso accetta, mediante dichiarazione o azione positiva inequivocabile, il trattamento dei dati personali che lo riguardano;

22) «comunicazione»: il dare conoscenza dei dati personali a uno o più soggetti determinati, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o interconnessione;

23) «diffusione»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

24) «registro delle attività di trattamento»: l'elenco dei trattamenti di dati in forma cartacea o telematica effettuati dal Titolare e dal Responsabile del trattamento secondo i rispettivi ambiti del trattamento;

25) «valutazione d'impatto sulla protezione dei dati»: procedura atta a descrivere il trattamento, a valutarne la necessità e proporzionalità e a garantire la gestione dei rischi per i diritti e le libertà degli interessati;

26) «violazione dei dati personali»: la violazione che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

27) «autorità di controllo»: l'autorità pubblica indipendente, istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE, incaricata di sorvegliare l'applicazione del Regolamento stesso, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Per l'Italia, l'Autorità di Controllo è individuata dal Codice nel Garante per la Protezione dei Dati Personali (art. 153 D.Lgs n. 196/2003);

28) «amministratori di sistema»: la figura professionale dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;

29) «istituto o ente di ricerca»: un organismo pubblico o privato per il quale la finalità di statistica o di ricerca scientifica risulta dagli scopi dell'istituzione e la cui attività scientifica è documentabile;

30) «società scientifica», un'associazione che raccoglie gli studiosi di un ambito disciplinare, ivi comprese le relative associazioni professionali;

31) «ricerca scientifica»: un progetto di ricerca istituito conformemente alle pertinenti norme etiche e metodologiche settoriali, in conformità delle buone prassi.

Art. 3
TIPOLOGIE DI DATI TRATTATI DALL'UNIVERSITA'

1. L'Università degli Studi di Milano (di seguito, per brevità, anche «l'Università» o «l'Ateneo») è un'istituzione pubblica, sede primaria di attività di ricerca e di formazione, che persegue le finalità di elaborazione critica e di diffusione delle conoscenze, di interazione tra le culture, di sviluppo delle competenze, di educazione e formazione della persona, di arricchimento culturale della società.

2. Per il perseguimento dei propri fini istituzionali l'Università tratta principalmente le tipologie di dati personali di seguito indicate.

a) Dati, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, compresi i soggetti di cui il rapporto di lavoro è cessato, o altro personale operante a vario titolo nell'Università quali, ad esempio, borsisti, tirocinanti, visitatori etc. Tali dati vengono trattati nell'ambito delle seguenti attività:
   - prove concorsuali / selezioni;
   - gestione del rapporto di lavoro;
   - formazione e aggiornamento professionale;
   - gestione di progetti di ricerca;
   - monitoraggio e valutazione della ricerca;
   - attività di trasferimento tecnologico;
   - politiche Welfare e per la fruizione di agevolazioni;
   - salute e sicurezza delle persone nei luoghi di lavoro;
   - accesso ad aree riservate e parcheggi di pertinenza dell'Ateneo;
   - smart working e telelavoro;
   - erogazione del servizio di telefonia fissa e mobile.

b) Dati, anche di natura particolare, relativi a studenti, ivi compresi coloro che hanno già terminato gli studi e categorie assimilate. Tali dati vengono trattati nell'ambito delle seguenti attività:
   - attività di orientamento;
   - erogazione dei test di ingresso e verifica dei requisiti di accesso;
   - erogazione del percorso formativo e gestione della carriera, dall'immatricolazione alla laurea;
   - erogazione di attività didattica ed esami in modalità remota;
   - attività di tirocinio e stage;
   - attività di job placement;
   - attività di orientamento;
   - attività connesse allo svolgimento delle elezioni studentesche e alla rappresentanza degli studenti negli organi di governo dell'Ateneo;
   - attività connesse alle associazioni di ex-alunni;
   - attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community;
   - rilevazioni statistiche e valutazione della didattica;
   - diffusione dell'elaborato finale o di elementi ad esso connessi;
   - riscontro a richieste inoltrate dall'Autorità Giudiziaria, dalle Forze dell'Ordine o da altre Pubbliche Amministrazioni;
   - servizi di tutorato, assistenza, inclusione sociale;
   - servizi di assistenza ai disabili e DSA;
   - servizi e attività per il diritto allo studio;
   - procedimenti disciplinari a carico di studenti.

c) Dati relativi alla didattica e alla ricerca (compresa la ricerca in ambito medico – sanitario).
d) Dati relativi alle attività gestionali interne all'Ateneo e alle attività svolte per conto terzi e dati connessi ad attività trasversali svolte anche in modalità telematica. Tali dati vengono trattati nell'ambito delle seguenti attività:

- gestione degli spazi;
- gestione delle postazioni;
- gestione degli organi e delle cariche istituzionali;
- gestione degli infortuni;
- servizi bibliotecari;
- servizi di protocollo e conservazione documentale;
- acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso;
- servizi di posta elettronica e strumenti di collaboration;
- servizi di didattica a distanza;
- servizi di proctoring e di svolgimento degli esami online;
- erogazione federata di servizi;
- erogazione del servizio Eduroam;
- accesso a servizi federati;
- tracciamento di informazioni non primarie e gestione della sicurezza cibernetica;
- svolgimento di concorsi e riunioni.

Si intendono comunque disciplinati dal presente Regolamento tutti i trattamenti di dati svolti dall'Università, anche se non presenti nell'elenco di cui sopra, che rientrino nello svolgimento dei compiti istituzionali dell'Ateneo o che siano ad esso prescritti da una norma di legge.

ART. 4
PRINCIPI GENERALI DEL TRATTAMENTO

1. Il trattamento dei dati personali viene effettuato dall'Università in applicazione dei principi previsti dall'art. 5 del Regolamento UE.

2. I dati personali oggetto di trattamento sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) esatti e, se necessario, aggiornati: a tal fine sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati; possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, a condizione dell'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato;
f) trattati in modo da garantire una adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

3. Tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, l'Università adotta misure tecniche e organizzative adeguate, in grado di comprovare il rispetto dei principi sopra enunciati.

4. I sistemi forniti ed i servizi erogati da tutte le strutture centrali IT sono configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali e identificativi, 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.

Art. 5
SENSIBILIZZAZIONE E FORMAZIONE

1. Al fine della corretta e puntuale applicazione della disciplina in materia di protezione dei dati personali e della sicurezza informatica, l'Università sostiene e promuove, con il coinvolgimento degli organi istituzionali dell'Ateneo competenti per materia, strumenti di sensibilizzazione (anche tramite attività di formazione in aula, webinar o linee guida) finalizzati a consolidare la consapevolezza del valore della protezione dei dati personali, nonché attività formative indirizzate al personale dell'Ateneo e attività informativa diretta a coloro che intrattengono rapporti con l'Ateneo.

Art. 6
BASE GIURIDICA DEL TRATTAMENTO

1. La base giuridica del trattamento consiste, in via alternativa:
- nell'esecuzione dei compiti di interesse pubblico e connessi all'esercizio di pubblici poteri attribuiti all'Ateneo da norme di legge o di regolamento;
- nell'adempimento di obblighi contrattuali di cui l'interessato è parte o nell'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- nell'adempimento di obblighi di legge a cui è soggetto l'Ateneo;
- al di fuori dei propri compiti istituzionali, nel perseguimento del legittimo interesse dell'Ateneo o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
- nella salvaguardia degli interessi vitali dell'interessato o di altra persona fisica.
- nel consenso dell'interessato, laddove previsto.

2. Qualora il trattamento sia basato sul consenso, l'Università informa previamente l'interessato e acquisisce il consenso con modalità atte a dimostrare che l'interessato ha prestato il proprio consenso, libero, consapevole, inequivocabile, al trattamento dei propri dati personali.
L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Art. 7
CIRCOLAZIONE DEI DATI ALL'INTERNO DELL'UNIVERSITA'

1. L'accesso ai dati personali da parte delle strutture amministrative, di servizio, didattiche e scientifiche e dei dipendenti dell'Università, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della libera circolazione delle informazioni all'interno dell'Ateneo, secondo il quale l'Università provvede all'organizzazione delle informazioni e dei dati a propria disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione.

2. Ogni richiesta d'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, debitamente motivata e connessa con lo svolgimento dell'attività inerente alla loro specifica funzione, è soddisfatta in via diretta e senza ulteriori formalità nella misura necessaria al perseguimento dell'interesse istituzionale, ferma restando la responsabilità del richiedente derivante dall'eventuale utilizzo improprio dei dati.

3. Laddove la richiesta fosse finalizzata ad un utilizzo ulteriore e/o diverso dei dati personali, il richiedente è tenuto a segnalarlo in maniera esplicita e formale nella richiesta, da valutare a cura del Designato ai sensi dell'Allegato al presente Regolamento, e l'autorizzazione sarà concessa o negata a seconda che il fine della richiesta rientri o meno nell'attività istituzionale dell'Università.

4. Ai fini dell'accesso ai dati sono equiparati alle strutture dell'Università organi quali il Collegio dei Revisori, il Nucleo di Valutazione, il Comitato Etico nonché tutti gli altri organi di Ateneo limitatamente ai dati necessari per lo svolgimento delle proprie funzioni

MODELLO ORGANIZZATIVO INTERNO-DIRITTI DELL'INTERESSATO-LA SICUREZZA DEI DATI

ART. 8

MODELLO ORGANIZZATIVO INTERNO E FIGURE DI RIFERIMENTO

1.Tenuto conto del modello organizzativo interno, le figure di riferimento per la protezione dei dati personali sono le seguenti:

a. Il Titolare
b. I Designati,
c. I Referenti privacy;
d. Il Responsabile della Protezione dei dati personali;
e. I soggetti Autorizzati al trattamento dei dati personali;
f. Gli Amministratori di sistema.

Art. 9

TITOLARE DEL TRATTAMENTO

1. L'Università degli Studi di Milano, nella persona del Rettore in qualità di legale rappresentante, è Titolare del trattamento dei dati personali trattati dalla stessa.

2. Tutti i Responsabili del trattamento e gli Autorizzati dell'Università degli Studi di Milano sono tenuti ad attenersi alle prescrizioni dell'Ateneo. Il mancato rispetto delle suddette prescrizioni potrebbe infatti comportare che sia i Responsabili del trattamento sia gli Autorizzati si trovino ad agire quali Titolari autonomi del trattamento, assumendone così i conseguenti obblighi e responsabilità, ivi compreso quanto previsto dal successivo Art- 36 comma 3 sull'eventuale risarcimento del danno erariale.
3. Quando l'Università determina finalità e mezzi del trattamento congiuntamente con un altro Titolare, assume, unitamente a quest'ultimo, il ruolo di Contitolare del trattamento.
4. I Contitolari definiscono in modo trasparente, mediante un accordo interno, i rispettivi ruoli e responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle Informazioni di cui al successivo art. 20. Il contenuto essenziale dell'accordo di Contitolarità è messo a disposizione dell'interessato, dietro richiesta.
5. L'interessato può esercitare i propri diritti nei confronti di ciascun Contitolare del trattamento.

Art. 10
DESIGNATO E REFERENTE DEL TRATTAMENTO DEI DATI PERSONALI

1. Il Titolare individua i Designati nei responsabili apicali di struttura di cui all'Allegato A, i quali hanno il compito di vigilare, monitorare e garantire, all'interno della struttura cui sono preposti, il rispetto delle norme vigenti e delle istruzioni del Titolare in materia di protezione dei dati personali.
2. I Designati possono individuare, all'interno della propria struttura, un Referente che avrà il compito di interfacciarsi con il Responsabile per la protezione dei dati personali di Ateneo per ogni comunicazione legata all'applicazione della normativa in materia di protezione dei dati personali e supportare il designato nella gestione delle attività relative al trattamento dei dati personali. Al Designato sono attribuite le responsabilità di indirizzo, vigilanza e controllo sull'operato del Referente. L'individuazione del soggetto Referente non libera il Designato in relazione ai suoi compiti di cui al comma 1.
3. I Referenti sono individuati dal Designato tra il personale tecnico-amministrativo della struttura, in possesso delle necessarie competenze professionali. Per i Dipartimenti, in base alla complessità ed eterogeneità dei dati trattati, il Designato può individuare il Referente anche tra il personale docente o ricercatore. I nominativi dei Referenti individuati devono essere comunicati, per via telematica, al Titolare e al Responsabile della Protezione dei dati personali.
4. Qualora i dati siano trattati su sistemi informatici amministrati centralmente dalla Direzione ICT, il Dirigente della stessa Direzione, oltre che come Designato, agisce anche come Referente.

Art. 11
RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DPO)

1. Il Titolare designa un Responsabile della Protezione dei Dati (DPO), figura individuata sulla base delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui al successivo comma 3, che svolge funzioni di raccordo con il Garante e di tutela degli interessati.

2. Il DPO può essere un soggetto interno all'Università, nominato con decreto rettorale, oppure un soggetto esterno, nel qual caso assolve i propri compiti in base a un contratto di servizi.

3. Il DPO, considerando i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo, svolge i seguenti compiti:
- informa e fornisce consulenza al Titolare, al Responsabile e ai soggetti Autorizzati in merito agli obblighi derivanti dal Regolamento UE e dalle altre disposizioni normative in materia di protezione dei dati personali;
- sorveglia l'osservanza della normativa e delle politiche dell'Università in materia di protezione dei dati personali - comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento;
- coopera con il Garante fungendo da punto di contatto per lo stesso per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- collabora alla redazione e all'aggiornamento dei Registri di trattamento;
- tiene i contatti con gli interessati, in relazione all'esercizio dei loro diritti.

Il Titolare può assegnare al DPO ulteriori compiti e funzioni, purché non diano adito a conflitti di interesse e non siano d'ostacolo all'adempimento delle relative responsabilità.

4. Il DPO ha ampio accesso alle informazioni ed è interpellato per ogni problematica inerente la protezione dei dati e per ogni attività che implica un trattamento di dati, fin dalla sua progettazione.

5. L'Università garantisce che il DPO eserciti le proprie funzioni in autonomia e indipendenza.

6. L'Università comunica al Garante il nominativo e i dati di contatto del DPO, li inserisce nelle Informazioni agli interessati e in tutti gli atti che contengano un trattamento di dati personali e li pubblica sul sito internet istituzionale.

Art. 12

SOGGETTI AUTORIZZATI AL TRATTAMENTO

1. Sono soggetti Autorizzati al trattamento tutti coloro i quali svolgono le operazioni inerenti al trattamento sotto la diretta autorità del Titolare e, in quanto tali, sono autorizzati a trattare i dati personali nel pieno rispetto delle istruzioni del Titolare.

2. Il personale dell'Ateneo è Autorizzato al trattamento nell'ambito definito dalle mansioni attribuite con contratto di lavoro o atto di nomina, dalle competenze della struttura di assegnazione o afferenza e dalle attività assegnate dal Responsabile di struttura.

3. Tutti i dipendenti dell'Ateneo sono tenuti a seguire le indicazioni e le disposizioni dell'Ateneo in materia di protezione dei dati personali e sicurezza informatica e ad agire in modo conforme alla normativa vigente anche quando svolgono attività lavorativa da remoto (smart working, lavoro agile o telelavoro).

Art. 13
AMMINISTRATORI DI SISTEMA

1. Sono Amministratori di sistema ai sensi del Provvedimento del Garante del 27 novembre 2008 e s.m.i le figure professionali finalizzate alla gestione e manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente regolamento sono da considerarsi tali anche gli amministratori di basi di dati, gli amministratori di rete, gli amministratori di apparati di sicurezza, gli amministratori di sistemi software complessi.

2. L'Amministratore di sistema sviluppa e gestisce l'impianto di elaborazione o i suoi componenti hardware e software mediante i quali vengono effettuati i trattamenti di dati personali applicando per i profili relativi alla sicurezza le direttive del Titolare.

3. Il Titolare individua gli amministratori di sistema con atto di designazione individuale che definisce analiticamente i compiti e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Art. 14
RESPONSABILE DEL TRATTAMENTO

1. Il Responsabile del trattamento è il soggetto esterno all'organizzazione dell'Università che esegue trattamenti per conto dell'Università stessa. L'Università, per il trattamento di dati personali, ricorre unicamente a Responsabili che presentino garanzie idonee, in particolare in relazione alle misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni del Regolamento UE, ivi compresa la tutela dei diritti degli interessati.

2. L'Università designa il Responsabile del trattamento mediante un contratto o altro atto giuridico che determina la natura, la durata e la finalità del trattamento o dei trattamenti assegnati, il tipo di dati trattati, le categorie di interessati, gli obblighi e i diritti del Titolare e del Responsabile, le responsabilità e le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal Titolare e delle disposizioni normative.

3. Obblighi specifici del Responsabile sono:

- la tenuta del Registro dei trattamenti svolti per conto del Titolare del trattamento;

- l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti;

- la designazione di un Responsabile della Protezione Dati, se prevista dalla legge o se ritenuta necessaria;

- la designazione di un rappresentante in Italia (nel caso di Responsabile non stabilito nella UE);

- il rispetto delle istruzioni fornite dal Titolare del trattamento.

4. Per specifiche attività di trattamento, nel rispetto degli obblighi contrattuali che lo legano all'Università, il Responsabile può nominare sub-responsabili del trattamento esclusivamente previa autorizzazione scritta, specifica o generale, dell'Università e con attribuzione al sub-responsabile dei medesimi obblighi in materia di protezione dei dati personali derivanti dal contratto – o altro atto giuridico – tra Università e Responsabile. Qualora un sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti dell'Università l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

5. L'Università può essere nominata Responsabile di uno o più trattamenti per conto di un altro Titolare.

Art. 15
PRIVACY BY DESIGN NELLA PROGETTAZIONE DEGLI IMPIANTI DI ELABORAZIONE DELL'ATENEO

1.Chiunque progetti o sviluppi impianti di elaborazione o suoi componenti hardware e software deve assicurare la rispondenza della soluzione alla normativa sul trattamento di dati personali sin dalla fase di progettazione e sviluppo dell'impianto, ivi compresi i profili relativi alla sicurezza.

Art. 16
DIRITTI DELL'INTERESSATO
1. L'Università garantisce i diritti degli interessati di cui agli artt. da 15 a 22 del Regolamento UE. In particolare, l'interessato può:

a) ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro comunicazione in forma intelligibile;
b) ottenere senza ingiustificato ritardo la rettifica dei dati inesatti e l'integrazione dei dati incompleti;
c) ottenere senza ingiustificato ritardo la cancellazione dei dati, nei casi e con i limiti previsti dal Regolamento UE;
d) ottenere la limitazione del trattamento nei casi e con gli effetti previsti dal Regolamento UE;
e) ricevere i dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad altro Titolare, se il trattamento si basa sul consenso e viene effettuato con mezzi automatizzati;
f) ottenere la trasmissione diretta dei dati dall'Università ad altro Titolare, nei casi previsti dalla lettera precedente e se tecnicamente fattibile;
g) opporsi al trattamento;
h) proporre reclamo a un'Autorità di controllo;
i) proporre ricorso all'Autorità Giudiziaria.

2. L'interessato, previa identificazione, può esercitare i diritti con richiesta al Titolare anche per il tramite del Responsabile della Protezione dei Dati dell'Ateneo secondo le seguenti modalità:

- di persona presso le strutture competenti a ricevere la richiesta in quanto trattano il dato (ad es. Segreterie Studenti, Direzione Risorse Umane)
- via pec a unimi@postecert.it indirizzandola alla struttura che tratta il dato;
- via e-mail, scrivendo a: dpo@unimi.it
- via pec all'indirizzo dpo@pec.unimi.it
- con apposita comunicazione inviata via posta all'Università degli Studi di Milano, Via Festa del Perdono 7 20122 – Milano. all'attenzione dell'ufficio Archivio e protocollo

3. L'istanza può essere presentata da un delegato dell'interessato, che esibisce o allega copia della procura o della delega sottoscritta, unitamente a copia fotostatica non autenticata di un documento di riconoscimento proprio e dell'interessato.

4. I diritti riferiti a dati personali di persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione. È fatto salvo il caso in cui l'interessato abbia manifestato in modo non equivoco la volontà specifica, libera e informata di vietare l'esercizio dei diritti o di alcuni di essi.

5. La richiesta dell'interessato viene soddisfatta senza ingiustificato ritardo e comunque nel termine massimo di 1 mese dal ricevimento della richiesta, prorogabile di ulteriori 2 mesi se necessario, tenuto conto della complessità e del numero delle richieste. L'interessato è informato della proroga e dei motivi del ritardo entro 1 mese dal ricevimento della richiesta. L'Università, dietro esplicita richiesta dell'interessato, informa della richiesta di cancellazione ogni altro Titolare che tratta i dati personali cancellati.

6. L'esercizio dei diritti è gratuito, salvi i casi di richieste manifestamente infondate o eccessive, anche per il loro carattere ripetitivo, per le quali potrà essere addebitato un contributo spese ragionevole in base ai costi amministrativi sostenuti dall'Università. In alternativa, in questi casi il Titolare è legittimato a rifiutarsi di soddisfare la richiesta, dimostrandone il carattere manifestamente infondato o eccessivo.

Art. 17 REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

1. L'Università, in qualità di Titolare del trattamento, istituisce un Registro delle attività di trattamento svolte sotto la propria responsabilità.
Il Registro contiene le seguenti informazioni:
a) la struttura competente in ordine al trattamento;
b) ove esistenti, i nominativi e i dati di contatto del/i Contitolare/i e del/i Responsabile/i del trattamento;
c) le finalità del trattamento;
d) una descrizione delle categorie di interessati e delle categorie di dati personali;
e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
f) l'eventuale trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, con l'indicazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
h) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
Per consentire al Titolare la tenuta del Registro, nel caso di inizio o cessazione di un trattamento, il Responsabile della struttura interessata, anche tramite il Referente eventualmente individuato, informa tempestivamente il Titolare e il DPO fornendo tutte le informazioni utili all'inserimento del trattamento nel Registro.

2. L'Università tiene altresì un Registro di tutte le categorie di trattamenti svolti in qualità di Responsabile per conto di altri Titolari di trattamento, contenente:
a) la struttura competente in ordine al trattamento;
b) il nominativo e i dati di contatto del Titolare per conto del quale l'Università agisce e del Responsabile della protezione dei dati;
c) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
d) l'eventuale trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, con l'indicazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
e) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

3. I Registri, tenuti in forma scritta, anche in formato elettronico, sono messi a disposizione del Garante o dei danti causa dietro motivata richiesta.

Art. 18
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università, prima di procedere al trattamento, effettua, consultandosi con il DPO, una valutazione dell'impatto sulla protezione dei dati personali. Può essere condotta una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Fatte salve le tipologie di trattamento individuate dal Garante, la valutazione d'impatto viene effettuata dall'Università nei seguenti casi:
a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo significativamente analogo su dette persone;

b) trattamento su larga scala di categorie particolari di dati personali di cui al successivo art. 23 o di dati relativi a condanne penali e a reati;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
d) trattamento di dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

3. La valutazione di impatto contiene i seguenti elementi:
a) una descrizione sistematica del trattamento e delle sue finalità;
b) una valutazione in ordine alla necessità e alla proporzionalità del trattamento in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte.

4. Se necessario, l'Università procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto, quando insorgono variazioni del rischio rappresentato dalle attività di trattamento.

5. I Designati, anche per il tramite dei Referenti, comunicano al Titolare tutti i nuovi trattamenti che intendono effettuare, per consentire allo stesso di effettuare, ove necessario, la valutazione di impatto.

ART. 19
CONSULTAZIONE PREVENTIVA

1. L'Università, per il tramite del DPO, prima di procedere al trattamento, consulta il Garante qualora la valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio.

2. Se ritiene che il trattamento previsto violi il Regolamento UE, in particolare qualora l'Università non abbia identificato o attenuato sufficientemente il rischio, il Garante fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto all'Università. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. Il Garante informa l'Università di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte del Garante delle informazioni richieste ai fini della consultazione.

3. In sede di consultazione, l'Università comunica al Garante:
a) le rispettive responsabilità dell'Università in qualità di Titolare, nonché di eventuali Contitolari e Responsabili del trattamento;
b) le finalità e i mezzi del trattamento;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
d) i dati di contatto del DPO;
e) la valutazione d'impatto sulla protezione dei dati;
f) ogni altra informazione richiesta dal Garante.

Art. 20
INFORMAZIONI ALL'INTERESSATO

1. L'Università, ogniqualvolta provvede alla raccolta di dati personali presso l'interessato, fornisce a quest'ultimo, laddove già non ne disponga e fatti salvi gli altri casi previsti dall'art. 14, comma 5, del Regolamento UE, le seguenti informazioni:
a) l'identità e i dati di contatto del Titolare del trattamento;
b) i dati di contatto del DPO;
c) le finalità e la base giuridica del trattamento;
d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e) l'eventuale intenzione del Titolare di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, con indicazione del fondamento giuridico del trasferimento (esistenza di una decisione di adeguatezza della Commissione Europea o garanzie appropriate o opportune) e indicazione dei mezzi per ottenere una copia dei dati o del luogo dove sono stati resi disponibili;
f) il periodo di conservazione dei dati personali oppure, se non è possibile indicare il periodo, i criteri utilizzati per determinarlo;
g) i diritti dell'interessato;
h) la natura obbligatoria o facoltativa della fornitura dei dati e le possibili conseguenze del mancato conferimento;
i) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione, con indicazioni sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

2. Se la raccolta dai dati non avviene presso l'interessato, l'Università fornisce al medesimo, in aggiunta alle indicazioni di cui al comma 1, le seguenti informazioni:
   a) categorie di dati trattati;
   b) fonte da cui i dati hanno origine.

L'Università fornisce tali informazioni:
- entro un termine ragionevole dall'ottenimento dei dati personali e, in ogni caso, entro un mese;
- se i dati sono finalizzati alla comunicazione con l'interessato, non oltre la prima comunicazione con lo stesso;
- se è prevista la comunicazione dei dati ad altro destinatario, non oltre la prima comunicazione al medesimo.

L'Università non è tenuta a fornire tali informazioni se:
- l'interessato ne dispone già;
- la comunicazione all'interessato risulta impossibile;
- la comunicazione all'interessato implica uno sforzo spropositato, in particolare nel caso di trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o a fini statistici, ferma restando l'adozione di garanzie adeguate per i diritti e le libertà dell'interessato e di misure tecniche e organizzative, come la pseudonimizzazione, che assicurino il rispetto del principio di minimizzazione dei dati;
- la comunicazione all'interessato rischia di pregiudicare gravemente il conseguimento delle finalità del trattamento, ferma restando l'adozione di misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
- l'ottenimento dei dati è espressamente previsto da norma comunitaria o nazionale che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato;
- i dati personali devono rimanere riservati per un obbligo di segreto professionale o un obbligo di segretezza previsto per legge.

3. Le informazioni sono fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, per iscritto, anche con mezzi elettronici, oppure oralmente, se richiesto dall'interessato.

4. Qualora l'Università intenda trattare i dati per una finalità differente da quella per cui sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

ART. 21
PRIVACY E SICUREZZA INFORMATICA

1. Tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche, il Titolare mette in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio, tutelino il patrimonio informativo dell'Ateneo e prevengano l'accadimento di incidenti di sicurezza. Tali misure sono testate e verificate regolarmente per garantire la sicurezza del trattamento, con facoltà per l'Ateneo di prescrivere correttivi e bloccare temporaneamente o definitivamente un trattamento e il sistema che concorre ad effettuarlo, fino al rientro in parametri di sicurezza accettabili.

2. Le misure di sicurezza sono descritte, unitamente alle direttive e alle procedure cui attenersi, sul sito di ateneo.

3. I Designati, i Referenti e ogni soggetto Autorizzato sono tenuti all'osservanza delle misure e delle indicazioni di cui al comma 2, che sono altresì oggetto della formazione prevista dall'art. 5.

Art. 22

VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

1. In caso di violazione dei dati personali, l'Università, con comunicazione del DPO, notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica al Garante non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. La notifica deve contenere i seguenti elementi:

a) natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti;

b) nome e dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;

c) probabili conseguenze della violazione dei dati personali;

d) misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

3. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

4. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università comunica la violazione all'interessato senza ingiustificato ritardo.

5. Non è richiesta la comunicazione all'interessato se ricorre una delle seguenti condizioni:

a) l'Università ha messo in atto le adeguate misure, tecniche e organizzative, di protezione (in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia Autorizzato ad accedervi, come la cifratura) e tali misure erano state applicate ai dati personali oggetto della violazione;

b) l'Università ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) la comunicazione richiederebbe sforzi sproporzionati, nel qual caso si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

6. Nel caso in cui l'Università non abbia comunicato all'interessato la violazione dei dati personali, il Garante, dopo aver valutato la probabilità che la violazione presenti un rischio elevato, può richiedere che vi si provveda o può decidere che una delle condizioni di cui al comma 5 è soddisfatta.

7. L'Università documenta qualsiasi violazione dei dati personali, le relative circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio.

8. Il Settore Cybersecurity supporta il Titolare coordinandosi con il DPO nella gestione dei data breach.

9. Il personale d'Ateneo è tenuto a conformarsi alle ulteriori regole e istruzioni che sono state adottate dall'Ateneo, soprattutto per quanto riguarda la comunicazione delle informazioni rilevanti e la cooperazione con gli uffici competenti nella gestione dei data breach.

10. Il Designato, anche avvalendosi del Referente eventualmente individuato, assicura, senza ingiustificato ritardo, l'invio a violazione.dati@unimi.it di tutte le informazioni utili alla gestione del data breach.

TIPOLOGIE DI TRATTAMENTO E MODALITA' DI DIFFUSIONE DI DATI PERSONALI

Art. 23
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

1. Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona è ammesso solo in presenza di una delle condizioni di seguito elencate:

a) l'interessato ha prestato il consenso esplicito per una o più finalità specifiche;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti dell'Università o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
c) il trattamento è necessario per tutelare un interesse vitale della persona interessata o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestatamente pubblici dall'interessato;
e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali e i dati sono trattati da o sotto la responsabilità di un professionista soggetto a segreto professionale;
g) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, in conformità dell'art. 89 paragrafo 1 del Regolamento UE;
h) il trattamento è necessario per motivi di interesse pubblico rilevante, se previsto dal diritto dell'Unione Europea o da una disposizione di legge o di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante,

nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Si considerano di rilevante interesse pubblico i trattamenti eseguiti nelle seguenti materie:
- accesso a documenti amministrativi e accesso civico;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- obiezione di coscienza;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
- compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
- tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
- istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materiale sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, tutela del patrimonio informativo dell'Ateneo, igiene e sicurezza di lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

3. I dati genetici, biometrici e relativi alla salute possono essere trattati solo in presenza di una delle condizioni di cui al comma 1 e in conformità alle misure di garanzia disposte dal Garante.

4. I dati genetici, biometrici e relativi alla salute non possono essere diffusi.

5. Nel rispetto degli obblighi riguardanti le misure di sicurezza a tutela dei dati personali, è ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti Autorizzati, nel rispetto delle misure di garanzia di cui all'art. 2-septies del Codice.

Art. 24

TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

1. Le strutture e i servizi dell'Università operanti in ambito sanitario o della prevenzione e sicurezza del lavoro, con esclusione di quelle di cui al successivo comma 5, trattano dati personali idonei a rivelare lo stato di salute se necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, gestione dei sistemi e servizi sanitari o sociali ovvero per motivi di interesse pubblico nel settore della sanità pubblica, sulla base di una norma di legge o di regolamento o del diritto dell'Unione Europea. Il trattamento è effettuato da un professionista soggetto al segreto professionale, o sotto la sua responsabilità, in conformità alle misure di garanzia disposte dal Garante e alle specifiche disposizioni di settore.

2. Le strutture e i servizi di cui al comma 1 possono adottare modalità semplificate per rilasciare le Informazioni sul trattamento dei dati personali, ivi compresi il rilascio delle Informazioni per una

pluralità di trattamenti di dati e l'apposizione di appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico.

3. Le Informazioni riguardanti il trattamento dei dati personali possono essere rese, senza ritardo, successivamente alla prestazione in caso di:
a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le Informazioni a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, familiare, convivente, unito civilmente, fiduciario o Responsabile della struttura presso cui dimora l'interessato;
b) rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato;
c) prestazione medica che può essere pregiudicata dal preventivo rilascio delle Informazioni, in termini di tempestività o efficacia.
Dopo il raggiungimento della maggiore età, le Informazioni sul trattamento dei dati personali sono fornite all'interessato, se non già rilasciate in precedenza.

4. Fermo restando quanto previsto dalle norme di legge e di regolamento in materia di trattamento di categorie particolari di dati personali e di misure di sicurezza, nei trattamenti di cui al comma 1 sono adottate le seguenti misure: distanze di cortesia; soluzioni che prevengano l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute; cautele per evitare l'erogazione di prestazioni in situazioni di promiscuità dovute a modalità o locali prescelti; accorgimenti volti ad assicurare che la notizia o conferma, anche telefonica, sia data ai soli terzi legittimati; rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento; sottoposizione a regole di condotta analoghe al segreto professionale di tutti coloro che effettuano trattamenti di dati personali in ambito sanitario.

5. Non rientrano nell'ambito di applicazione del comma 1 le strutture universitarie afferenti alla Facoltà di Medicina e Chirurgia convenzionate con il Servizio Sanitario Nazionale, che trattino i dati per conto dell'Azienda ospedaliera di accreditamento, Titolare del trattamento. Rispetto a dette strutture trovano applicazione le leggi e i regolamenti che disciplinano i trattamenti di dati personali da parte degli organismi sanitari pubblici, nonché le disposizioni impartite dall'Ente Ospedaliero.

Art. 25

TRATTAMENTO DI DATI RELATIVI A CONDANNE PENALI E REATI

1.Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è ammesso solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che preveda garanzie appropriate per i diritti e le libertà degli interessati, in particolare nei seguenti casi:

a) adempimento di obblighi ed esercizio di diritti da parte del Titolare o dell'interessato nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento;
b) adempimento di obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione di controversie civili e commerciali;
c) verifica o accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
d) accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
e) accertamento, esercizio o difesa di un diritto in sede giudiziaria;
f) esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
g) adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di

pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;

h) accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
i) adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Art. 26
TRATTAMENTO DI DATI PERSONALI PER LA GESTIONE DEL RAPPORTO DI LAVORO

1. L'Università effettua il trattamento dei dati personali dei dipendenti per finalità di assunzione esecuzione del contratto di lavoro – compreso l'adempimento degli obblighi stabiliti dalla legge e da contratti collettivi -, gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto d lavoro, salute e sicurezza sul lavoro, protezione della proprietà e del patrimonio informativ dell'Ateneo, cessazione del rapporto di lavoro.

2. Il trattamento non richiede il consenso dell'interessato, in quanto necessario per assolvere gli obbligh ed esercitare i diritti del Titolare e dell'interessato in materia di diritto del lavoro, sicurezza protezione sociale.

3. Il trattamento di dati personali nell'ambito del rapporto di lavoro è effettuato adottando garanzi appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui, iv comprese le prerogative individuali e sindacali previste dallo Statuto dei Lavoratori e dalle regol deontologiche promosse dal Garante.

Art. 27
TRATTAMENTO DEI DATI PERSONALI NELLE SEDUTE DEGLI ORGANI COLLEGIALI

1. Nelle sedute degli Organi Collegiali dell'Università, il trattamento dei dati personali avviene in conformità al presente Regolamento e al solo fine dello svolgimento, da parte dei componenti degli Organi, delle attività istruttorie necessarie per le finalità deliberative di competenza degli stessi.

ART. 28

TRATTAMENTO A FINI DI ARCHIVIAZIONE, DI RICERCA SCIENTIFICA O STORICA E A FINI STATISTICI

1.L'Università, nel trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica e a fini statistici, predispone misure tecniche e organizzative che garantiscano il rispetto del principio della minimizzazione dei dati, ivi inclusa la pseudonimizzazione e l'anonimizzazione, se le finalità del trattamento possono essere raggiunte mediante tali misure.

2.Il trattamento per le finalità di cui al comma 1 è effettuato anche oltre il periodo di tempo necessario per conseguire gli scopi per i quali i dati sono stati in precedenza raccolti o trattati. Per tali finalità, l'Università può conservare o cedere ad altro Titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento, nel rispetto delle misure di cui al comma 1.

3.Nell'ambito delle proprie finalità istituzionali, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, l'Università può comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca,

tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione delle categorie particolari di dati personali e dei dati relativi a condanne penali e reati.

ART. 29
TRATTAMENTO PER FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE O DI RICERCA STORICA

1. Fatto salvo quanto previsto dal precedente art. 28, i dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non sono utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità secondo i principi stabiliti dall'art. 5 del Regolamento UE.

2. I documenti contenenti dati personali trattati a fini di archiviazione nel pubblico interesse o di ricerca storica sono utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il raggiungimento di tali scopi. I dati personali diffusi sono utilizzati solo per il perseguimento dei medesimi scopi.

3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o da suoi comportamenti in pubblico.

4. Il trattamento è effettuato nel rispetto delle regole deontologiche in materia approvate dal Garante.

5. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dal d. lgs. n. 42/2004 e dalle relative regole deontologiche.

ART. 30
TRATTAMENTO A FINI STATISTICI O DI RICERCA SCIENTIFICA

1. Fermo restando quanto previsto dall'art. 28, i dati personali trattati a fini statistici o di ricerca scientifica non sono utilizzati per prendere decisioni o provvedimenti relativamente all'interessato né per trattamenti per scopi di altra natura.

2. Le Informazioni rese all'interessato devono chiaramente evidenziare le finalità statistiche e di ricerca scientifica e possono essere rese anche al familiare o convivente dell'interessato, che risponde in suo nome e per suo conto, quando le circostanze lo consentono. Le Informazioni non sono dovute quando richiedono uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate dalle regole deontologiche in materia, promosse dal Garante.

3. Al di fuori dei casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di categorie particolari di dati personali, quando richiesto, può essere presentato con modalità semplificate, individuate dalle regole deontologiche o dalle misure di garanzia disposte dal Garante.

ART. 31
TRATTAMENTO A FINI DI RICERCA MEDICA, BIOMEDICA ED EPIDEMIOLOGICA

1. Fermo restando quanto previsto dall'art. art. 28, il consenso dell'interessato al trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico ed epidemiologico non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione Europea - ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'art. 12 bis del d. lgs. n. 502/1992 - ed è condotta e resa pubblica una valutazione d'impatto.

2. Il consenso al trattamento non è necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il Titolare adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato; il programma di ricerca è oggetto di motivato parere favorevole del Comitato Etico a livello territoriale e deve essere sottoposto a valutazione d'impatto sulla protezione dei dati secondo quanto previsto dall'art. 18 del presente Regolamento.

3. In caso di esercizio del diritto di rettifica e integrazione dei dati personali da parte dell'interessato, la rettificazione e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

Art. 32
COMUNICAZIONE E DIFFUSIONE DI DATI PERSONALI

1. L'Università può comunicare e diffondere dati personali, diversi da quelli particolari e relativi a condanne penali e reati, nei seguenti casi:

- comunicazione fra Titolari che effettuano trattamenti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, se previsto da norme di legge, di regolamento o dal diritto dell'Unione Europea. In mancanza di tali norme, la comunicazione è ammessa se necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata decorso il termine di quarantacinque giorni dalla comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure a garanzia degli interessati;

- comunicazione e diffusione necessarie per finalità di difesa o sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia;

- comunicazione e diffusione necessarie per il soddisfacimento di richieste di accesso ai sensi dell'art. 22 della legge 241/90;

- comunicazione e diffusione, anche su richiesta di privati e per via telematica, di dati relativi agli esiti formativi intermedi e finali di studenti, diplomati, laureati, specializzati, borsisti, dottorandi, assegnisti e altri profili formativi, nonché di soggetti che hanno superato l'esame di Stato, e di altri dati personali comuni pertinenti in relazione alla finalità di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, degli studenti e dei laureati dell'Ateneo, anche mediante inviti ad incontri, manifestazioni, riunioni e congressi;

- comunicazione a finanziatori di borse di dottorato e di assegni alla ricerca di dati personali relativi a dottorandi e assegnisti che abbiano usufruito dei finanziamenti;

- comunicazione ad altre pubbliche amministrazioni e diffusione, anche sui siti web di Ateneo dei nominativi del personale e dei collaboratori dell'Università, del ruolo ricoperto, dei recapiti telefonici e degli indirizzi telematici istituzionali, al fine di favorire la comunicazione istituzionale;

- comunicazione ad enti pubblici e privati di dati necessari alla gestione del rapporto di lavoro relativi al personale trasferito, comandato, distaccato o comunque assegnato in servizio a un ente diverso da quello di appartenenza;

- comunicazione alle Aziende Ospedaliere in convenzione di dati personali inerenti il personale universitario che eserciti la propria attività nell'ambito della convenzione con tali Enti;

- comunicazione a soggetti pubblici e privati che organizzano e gestiscono corsi di formazione di dati comuni del personale che partecipa a tali corsi.

2. Le richieste rivolte all'Università per ottenere la comunicazione o la diffusione di dati personali devono essere indirizzate per iscritto al Responsabile di struttura e devono contenere:

- il nome, la denominazione o la ragione sociale del richiedente;

- i dati cui la domanda si riferisce, le finalità e le modalità di utilizzo dei dati richiesti;

- l'eventuale ambito di comunicazione dei dati richiesti;

- la dichiarazione che il richiedente si impegna a utilizzare i dati ricevuti esclusivamente per le finalità e nell'ambito delle modalità per cui sono stati richiesti.

3. Sono escluse la comunicazione e la diffusione di categorie particolari di dati personali di studenti, laureati e altri profili formativi.

4. L'Università rilascia a terzi certificati contenenti dati personali relativi a studenti o laureati dell'Ateneo, previa esibizione di delega sottoscritta dall'interessato, accompagnata da copia fotostatica di un documento d'identità del delegante e del delegato.

5. L'Università pubblica sui siti web d'Ateneo gli esiti delle prove concorsuali e selettive e le relative graduatorie, nel rispetto del principio di minimizzazione dei dati, mediante diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati.

6. L'Università può comunicare e diffondere dati anonimi o aggregati per finalità di ricerca scientifica o di statistica.

ART. 33
COMUNICAZIONE E DIFFUSIONE DI DATI RELATIVI AD ATTIVITA' DI RICERCA

1. Nell'ambito delle proprie finalità istituzionali, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, l'Università può comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei dati appartenenti a categorie particolari e dei dati relativi a condanne penali e reati.

2. L'Università può comunicare informazioni inerenti la produttività scientifica, i riconoscimenti e i fondi acquisiti da singoli, gruppi o specifici settori scientifico-disciplinari, anche nell'ambito di procedure di valutazione di richieste di finanziamento o di progetti di ricerca, al fine di:

- promuovere modelli di programmazione delle attività di ricerca e di allocazione delle risorse secondo meccanismi che consentano di garantire trasparenza nella definizione delle priorità, di valorizzare adeguatamente le capacità dei singoli e dei gruppi e di rispettare i principi di trasparenza ed equità di trattamento;
- favorire la cooperazione tra singoli e gruppi mediante una precisa conoscenza dei risultati conseguiti, allo scopo di migliorare la capacità di attrarre finanziamenti esterni o di istituire forme di collaborazione strutturata con soggetti terzi;
- fornire orientamento e sostegno per lo sviluppo di modelli organizzativi di supporto alla ricerca, anche tramite la realizzazione di analisi comparative e la condivisione di buone pratiche.

3. L'Università può comunicare dati personali a soggetti pubblici che abbiano erogato dei finanziamenti per la ricerca, ai fini di rendicontazione e per consentire elaborazioni statistiche.

Art. 34

VIDEOSORVEGLIANZA

1. Il trattamento di dati personali attraverso sistemi di videosorveglianza da parte dell'Università avviene esclusivamente nell'ambito dello svolgimento delle funzioni istituzionali, per finalità di: a) sicurezza e incolumità del personale universitario, degli studenti e dei frequentatori a vario titolo degli spazi universitari e delle residenze; b) tutela del patrimonio immobiliare dell'Ateneo; c) tutela dei beni mobili dell'Università e degli utenti; d) prevenzione di atti vandalici; accesso a varchi o proprietà di diretta pertinenza dell'Ateneo.

2. Il trattamento viene effettuato, secondo le disposizioni del Regolamento d'Ateneo in materia di videosorveglianza, nel rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati e in osservanza dei principi di necessità e proporzionalità.

3. Laddove dalla valutazione d'impatto, per la natura dei dati trattati, per le modalità di trattamento o per gli effetti che il trattamento può determinare, emergano rischi specifici per i diritti e le libertà fondamentali degli interessati, l'Università chiede al Garante una consultazione preventiva. Resta ferma la necessità di effettuare una valutazione di impatto ogniqualvolta vengano installati sistemi di videosorveglianza su larga scala in ambienti o zone accessibili al pubblico.

4. Nelle strutture dove sono in funzione sistemi di videosorveglianza, deve essere affissa, in modo visibile dall'interessato e prima di entrare nel raggio d'operatività delle videocamere, apposita informativa che informi il pubblico della presenza degli impianti, del nominativo del Titolare del trattamento e delle finalità perseguite.

5. L'Università garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza mediante:
- la limitazione dell'accesso alle immagini ai soggetti appositamente Autorizzati;
- la formazione specifica sulla protezione dei dati del personale coinvolto nelle operazioni di registrazione, visualizzazione e conservazione delle immagini e del personale addetto alla manutenzione degli impianti;
- la conservazione delle immagini per il solo tempo necessario a raggiungere le finalità perseguite e in ogni caso per un tempo massimo di **3 giorni** dalla rilevazione, fatti salvi i casi di specifiche richieste investigative dell'autorità giudiziaria o di polizia giudiziaria, nonché le ipotesi di chiusura programmata dell'Ateneo o esigenze particolari legate a determinati impianti che potrebbero richiedere tempi di conservazione inferiori o superiori,
- l'applicazione di misure di sicurezza adeguate al livello di rischio finalizzate a ridurre i rischi di distruzione, perdita anche accidentale, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Art. 35
DIRITTO DI ACCESSO E RISERVATEZZA

1. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e la relativa tutela sono disciplinati dalla L. n. 241/1990 e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che riguarda le categorie particolari di dati e i dati relativi a condanne penali e reati.

2. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico sono disciplinati dal D. lgs. n. 33/2013.

3. L'esercizio del diritto d'accesso, qualora comporti la comunicazione di dati personali di terzi, deve essere limitato ai dati necessari a soddisfare il diritto stesso. Resta fermo il principio per cui i conflitti tra diritto di accesso e riservatezza dei terzi devono essere risolti nel senso che l'accesso, finalizzato alla cura o alla difesa di propri interessi legittimi, prevale rispetto all'esigenza di riservatezza, nei limiti in cui esso è necessario alla difesa di un interesse giuridicamente rilevante.

4. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, 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.

NORME FINALI

Art. 36
AMBITO DELLA RESPONSABILITA'

1. L'Università degli Studi di Milano, in qualità di Titolare del trattamento, è responsabile del danno materiale o immateriale causato dal trattamento stesso in violazione delle disposizioni del Regolamento UE e del Codice, salvo che dimostri che l'evento dannoso non le è in alcun modo imputabile.

2. L'Università degli Studi di Milano, in qualità di Responsabile del trattamento, è responsabile del danno causato dal trattamento solo se non ha adempiuto gli obblighi del Regolamento UE e del Codice specificatamente diretti ai Responsabili del trattamento o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare, salvo che dimostri che l'evento dannoso non le è in alcun modo imputabile.

3. Qualora l'Università degli Studi di Milano dovesse essere sanzionata per azioni od omissioni correlate alla violazione delle norme e istruzioni sulla protezione dei dati, la cui responsabilità sia ascrivibile esclusivamente a un suo dipendente, valuterà se sussistono i presupposti per contestare il danno erariale e agire nelle sedi competenti sia per quanto riguarda l'aspetto patrimoniale sia per quanto riguarda l'aspetto disciplinare.

4. La responsabilità penale specificamente prevista dal Codice resta a carico della singola persona cui l'uso illegittimo sia imputabile.

Art. 37

STRUTTURA REFERENTE PER L'ESECUZIONE DEL REGOLAMENTO

La struttura dell'Ateneo referente per l'attuazione del presente Regolamento, indicazioni, modulistica e informazioni utili per l'attuazione sono reperibili alla pagina https://www.unimi.it/it/ateneo/normative/privacy.

Art. 38
ENTRATA IN VIGORE E REVISIONE DEL REGOLAMENTO

1. Il presente Regolamento ed eventuali successive modifiche sono deliberati dal Consiglio di Amministrazione, previo parere favorevole del Senato Accademico, sono emanati con decreto del Rettore ed entrano in vigore il quindicesimo giorno dalla pubblicazione sul sito web d'Ateneo. La presente procedura non si applica alla modifica di cui all'Allegato A al presente regolamento.

2. Per quanto non espressamente previsto dal presente Regolamento, si rinvia alle disposizioni del Regolamento UE e della normativa nazionale rilevante, oltre a quanto previsto dalle Regole deontologiche approvate dal Garante e dalla normativa d'Ateneo in materia di protezione dei dati personali.