UOR: Direzione Generale – Ufficio Relazioni con il Pubblico, Ufficio di supporto al RPD

Responsabile del Procedimento: dott.ssa Maria Bramanti

Estensore: dott.ssa Francesca di Perna

## IL RETTORE

VISTO il Decreto del Ministero dell'Università e della Ricerca Scientifica e Tecnologica del 10 giugno 1998, che ha istituito l'Università degli Studi di Milano – Bicocca;

VISTA la Legge 30 dicembre 2010, n. 240, "*Norme in materia di organizzazione delle università, di personale accademico e reclutamento, nonché delega al Governo per incentivare la qualità e l'efficienza del sistema universitario*";

VISTO l'art. 4 dello Statuto dell'Università degli Studi di Milano – Bicocca, emanato con D.R. n. 0012034/12 del 4 maggio 2012 e modificato con D.R. n. 0010332/15 del 3 marzo 2015;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale Sulla Protezione Dei Dati - GDPR);

VISTO il Decreto Legislativo 30 giugno 2003, n. 196, "*Codice in materia di protezione dei dati personali*", così come modificato dal Decreto Legislativo 10 agosto 2018, n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*";

VISTO il Provvedimento del Garante n. 243 del 15 maggio 2014 "*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*" pubblicato sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014;

VISTO lo Schema di Regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679, aggiornato al 23 ottobre 2018, approvato dalla CRUI;

VISTE le Linee guida CODAU in materia di privacy e protezione dei dati personali in ambito universitario del novembre 2017;

RILEVATO CHE l'Università degli Studi di Milano – Bicocca, al pari di altri Enti Pubblici, si trova a trattare quotidianamente dati personali, e categorie particolari di dati, identificativi di un considerevole numero di soggetti interessati;

CONSIDERATO CHE in vista della venuta ad efficacia del Regolamento è stato avviato un processo di adeguamento alla normativa, in primo luogo con la nomina di un Responsabile della Protezione dati con Delibera del Consiglio di Amministrazione n. 228/2018/CdA del 24/04/2018;

PRESO ATTO delle attività attuate in Ateneo in ragione della normativa, che si sostanziano nella consulenza specifica, nella formazione del personale, nella redazione di modulistica e linee guida in materia, nonché tutte le altre attività, tra cui anche quelle atte a riscontrare le istanze presentate e a fronteggiare le violazioni di dati;

RITENUTO CHE il Regolamento per il trattamento dei dati sensibili e giudiziari, attualmente in vigore in Ateneo, non è più rispondente alla normativa vigente in materia e si rende pertanto necessario l'emanazione di un nuovo Regolamento Interno che disciplini compiutamente il trattamento e la protezione dati;

VALUTATA la necessità di emanare un Regolamento che disciplini il trattamento e la protezione dei dati personali e della libera circolazione degli stessi presso l'Università di Milano Bicocca, in ragione della normativa vigente;

VALUTATA ALTRESÌ la necessità di emanare un atto regolamentare che preveda in maniera chiara e specifica anche l'organizzazione interna dell'Ateneo, in relazione al trattamento e protezione dati, definendo la ripartizione di ruoli e responsabilità;

VISTA la delibera adottata dal Consiglio di Amministrazione in data 20 novembre 2018, con la quale il Regolamento Interno per il trattamento e la protezione dei dati è stato approvato;

**DECRETA**

l'emanazione del "Regolamento per il trattamento e la protezione dei dati personali" dell'Università degli Studi di Milano – Bicocca, nel testo che segue.

## REGOLAMENTO PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

# INDICE

**Indice degli Acronimi**

- **CDA:** Consiglio d'Amministrazione
- **CNS**: Carta nazionale dei servizi
- **DPIA:** Data Protection Impact Assessment – Valutazione d'impatto
- **FEA:** Firma elettronica avanzata
- **GDPR:** General Data Protection Regulation – Regolamento UE 2016/679
- **GFM**: Firma avanzata grafometrica
- **OTP**: One-time password - codice password temporaneo
- **PDL**: postazioni di lavoro
- **PQA:** Presidio di Qualità d'Ateneo
- **RPD**: Responsabile per la protezione dei dati
- **SPID:** Servizio Pubblico d'Identità Digitale
- **U.U.O.O.R.R./U.O.R.**: Unità Operative Responsabili/Unità Operativa Responsabile
- **URP**: Ufficio Relazioni con il Pubblico

## 1. Premessa

Dopo un iter durato circa quattro anni, il 14 aprile 2016 l'Assemblea plenaria del Parlamento Europeo ha adottato il Regolamento Europeo in materia di protezione dei dati personali (di seguito GDPR), che ha abrogato la Direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Il GDPR 2016/679 mira ad introdurre una legislazione in materia di trattamento e protezione dati uniforme e valida in tutta Europa, affrontando temi innovativi e fissando criteri che responsabilizzano maggiormente Imprese ed Enti rispetto alla protezione dei dati personali, stabilendo norme comuni e standardizzate per il trattamento e la protezione dei dati valide all'interno di tutti gli Stati membri, con lo scopo di innalzare le garanzie per la privacy dei cittadini e di facilitare notevolmente lo scambio e l'uso delle informazioni utili.

Il nuovo GDPR lascia gli Stati membri liberi di adattare, quando possibile, i principi e le disposizioni previste con quelli applicati nelle singole legislazioni nazionali.

Per quanto riguarda il nostro Paese, con il D.Lgs. 101/2018, in vigore dal 19/09/2018, il legislatore ha armonizzato il Codice Privacy alle previsioni del Regolamento europeo, recependo *in toto* i principi.

Il diritto alla privacy è un vero e proprio diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti, delle libertà fondamentali e della dignità. Per questi motivi è necessario che la cultura della privacy cresca e si rafforzi, perché solo grazie alla conoscenza dei principi fondamentali che stanno alla base della vigente normativa, potranno essere correttamente adempiute tutte le previsioni di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente a migliorare i rapporti con l'utenza e i servizi ad essa offerti.

## 2. Scopo

Il presente documento è uno strumento di applicazione del GDPR nell'ambito dell'organizzazione dell'Ateneo, frutto di un'attenta analisi delle problematiche concrete che quotidianamente emergono nella tutela della riservatezza dei dati personali nei vari ambiti di competenza e di un lungo e approfondito studio della normativa vigente.

La stesura del Regolamento nasce, infatti, dall'esigenza di riorganizzare la disciplina in argomento all'interno dell'Università degli Studi di Milano-Bicocca (d'ora in avanti Università di Milano-Bicocca) al fine di recepire i principi fondamentali della nuova normativa europea, di definire i livelli di responsabilità in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, di individuare e definire i ruoli e le figure dell'Ateneo coinvolte nei processi di gestione dei dati stessi e di porre in essere tutte le misure tecnico-organizzative previste dal GDPR.

## 3. Campo di applicazione

Il presente Regolamento, adottato in attuazione del GDPR, disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi presso l'Università di Milano Bicocca.
L'Ateneo, in qualità di Titolare del trattamento, effettua i trattamenti di dati con o senza ausilio di processi automatizzati e nel rispetto dei diritti, delle libertà fondamentali, della dignità e del diritto alla riservatezza dell'Interessato.
I trattamenti effettuati dall'Università per il raggiungimento dei propri fini istituzionali non necessitano del consenso dell'Interessato, salvo alcune peculiari ipotesi che meglio verranno descritte di seguito nell'art. 17.
In questo contesto, il D.Lgs. 196/2003 aveva ben definito la gerarchia in materia di gestione della privacy, prevedendo le figure fondamentali da individuare all'interno dei singoli Enti:

- Titolare: la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione o Organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- Responsabile: la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione o Organismo preposti dal Titolare al trattamento di dati personali.
- Incaricato: la persona fisica autorizzata dal Titolare o dal Responsabile a compiere operazioni di trattamento.

L'impianto organizzativo sopra descritto, seppur non riproposto fedelmente dal GDPR, risulta ormai consolidato e funzionale alla gestione della protezione dei dati personali in Ateneo.
Il legislatore europeo, definiti il perimetro di azione, le nuove figure coinvolte e i nuovi concetti finalizzati al corretto trattamento dei dati personali e della tutela delle persone fisiche, consente agli Enti, in piena autonomia, di organizzarsi al fine di ottemperare agli obblighi previsti.
L'Università di Milano – Bicocca, pertanto, ha ritenuto necessario formalizzare, secondo lo schema delineato, i ruoli e le responsabilità dei soggetti coinvolti nei processi di protezione dei dati personali, rispettando i principi del GDPR.

## 4. Definizioni

Di seguito un glossario nel quale si indicano i riferimenti e le relative definizioni in relazione al presente Regolamento. S'intende per:

1. "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, 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;

2. "dato personale": qualunque informazione riguardante una persona fisica indentificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
3. "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 atti a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale;
4. "dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona stessa;
5. "dati biometrici": i dati personali ottenuti da un trattamento tecnico 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;
6. "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;
7. "dati giudiziari": dato idoneo a rivelare i provvedimenti giudiziaria carico dell'interessato di natura penale, civile o amministrativa.
8. "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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
9. "Responsabile per la protezione dei dati": figura specializzata nel supporto al Titolare del trattamento, prevista come obbligatoria negli enti pubblici (d'ora in avanti, anche RPD);
10. "Responsabile esterno 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;
11. "Responsabili interni del trattamento (Designati)": i soggetti che coadiuvano il Titolare nella definizione delle finalità, delle modalità di trattamento e dei mezzi atti a garantire l'osservanza della normativa europea sulla protezione dei dati personali. Questi sono i Responsabili delle UU.OO.RR.– Dirigenti d'Area, Direttori di Dipartimento, Direttori dei Centri di Ricerca, Medico competente, Prorettori, Delegati del Rettore, Responsabile scientifico (qualora, nell'ambito della propria attività di ricerca tratti dati personali la cui titolarità è dell'Ateneo gestendoli su server dell'Ateneo stesso), nonché tutte le altre figure a queste affini. Questi, per la propria area di competenza, garantiscono, insieme al Titolare, l'osservanza della normativa europea sulla protezione dei dati personali;
12. "Referenti per protezione dei dati": figure che hanno il compito di supportare il Responsabile in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il RPD e con l'Ufficio di supporto al RPD per tutte le attività relative alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia;

13. "Responsabile della transizione al digitale": soggetto i cui compiti sono definiti dall'art. 17, c. 1-sexies del Codice dell'Amministrazione Digitale (emanato con D.Lgs. n.82 del 7 marzo 2005, quale risultante dalle successive modifiche e integrazioni);
14. "Responsabile della conservazione dei documenti informatici": soggetto i cui compiti sono definiti dall'art. 44 del Codice dell'Amministrazione Digitale (emanato con D.Lgs. n.82 del 7 marzo 2005, quale risultante dalle successive modifiche e integrazioni);
15. "Amministratore di sistema": la figura professionale 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, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
16. "Autorizzati al trattamento": le persone fisiche che hanno accesso ai dati personali e trattano gli stessi a seguito di autorizzazione e secondo le istruzioni ricevute dal Titolare del trattamento;
17. "Interessato al trattamento": la persona fisica a cui si riferiscono i dati personali;
18. "consenso dell'Interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva, a che i dati personali che lo riguardano siano oggetto di trattamento;
19. "Terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del trattamento, il Responsabile del trattamento e gli Autorizzati al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
20. "Destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerati destinatari. Il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
21. "profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali 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;
22. "processo decisionale automatizzato": decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti nella sfera giuridica dell'Interessato o che incidono in modo analogo significativamente sullo stesso.
23. "pseudoniminizzazione": 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 tale attribuzione identificativa non possa avere luogo;
24. "limitazione di trattamento": il contrassegno dei dati personali, conservati con l'obiettivo di limitarne il trattamento in futuro;
25. "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;

26. "registro attività di trattamento": elenco dei trattamenti di dati in forma cartacea o telematica effettuati dal Titolare e dal Responsabile per la protezione secondo le rispettive competenze;
27. "valutazione d'impatto sulla protezione dei dati": procedura atta a descrivere il trattamento, valutarne le necessità e proporzionalità, e a garantire la gestione dei rischi dei diritti e delle libertà delle persone fisiche legate al trattamento dei loro dati personali;
28. "violazione dei dati personali": la violazione della sicurezza 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;
29. "Autorità di controllo": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
30. "trattamento transfrontaliero": trattamento di dati personali che ha luogo nell'ambito dell'attività di stabilimenti in più di uno Stato membro di un Titolare del trattamento o Responsabile del trattamento nell'Unione ove il Titolare del trattamento o il Responsabile del trattamento siano stabiliti in più di uno Stato membro; trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare del trattamento o Responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;
31. "Autorità di controllo interessata": l'Autorità di controllo competente in quanto: a) il Titolare o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale Autorità di controllo; b) gli Interessati che risiedono nello stato membro dell'Autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale Autorità di controllo;
32. "Organizzazione internazionale": un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

## 5. Le figure coinvolte

Le figure coinvolte nei processi di trattamento dei dati personali sono descritte nei seguenti paragrafi.

### 5.1 Titolare

Il Titolare del trattamento è definito al par. 7 dell'art. 4 del GDPR come "*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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*".

Nell'ambito del presente regolamento Titolare del trattamento di tutti i dati personali è l'Università di Milano - Bicocca, intesa come persona giuridica, rappresentata dal suo Legale Rappresentante, il Magnifico Rettore pro tempore. I dati di contatto del Titolare sono pubblicati sul sito internet istituzionale, nell'apposita sezione denominata "Protezione dati personali".

### 5.1.1. Compiti e Responsabilità

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR:

- liceità, correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza dei dati;
- limitazione della conservazione;
- integrità e riservatezza.

Il Titolare deve mettere in atto le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR. Tali misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'Interessato stabiliti dagli articoli da 15 a 22 del GDPR.

Il Titolare, in particolare, deve:

- fornire all'Interessato le informazioni relative al trattamento dei dati che lo riguardano, ai sensi degli artt. 13 e 14 del GDPR;
- effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (in seguito anche DPIA da *Data Protection Impact Assessment*), nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, come previsto dall'art. 35 del citato GDPR.

  La DPIA è condotta prima di dar luogo al trattamento, attraverso la descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta eventualmente approvati, della valutazione circa la necessità e proporzionalità dei trattamenti, sulla base delle finalità specifiche, esplicite e legittime, della liceità del trattamento, dell'adeguatezza, pertinenza e limitazione dei dati a quanto necessario, del periodo limitato di conservazione, delle informazioni fornite agli Interessati, del diritto di accesso, del diritto di rettifica, di opposizione e limitazione del trattamento, dei rapporti con i Responsabili del trattamento (art. 28). Il Titolare deve effettuare altresì la valutazione dei rischi per i diritti e le libertà degli Interessati, individuando le misure previste al fine di prevenirli, affrontarli e attenuarli, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento al GDPR, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione. Il Titolare si avvale della consulenza del RPD per definire la necessità di condurre o meno una DPIA, per individuare la metodologia da adottare e le misure tecniche e organizzative da mettere in atto al fine di attenuare i rischi delle persone interessate nonché per verificare la sua corretta esecuzione e la conformità degli esiti raggiunti con la normativa vigente;
- redigere il Registro delle attività di trattamento. Ai sensi dell'art. 30 ogni Titolare del trattamento deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro deve contenere tutte le informazioni relative a:

- il nome e i dati di contatto del Titolare del trattamento e, quando presente, del ConTitolare del trattamento;
- dati di contatto del RPD;
- le finalità del trattamento;
- le categorie di Interessati;
- le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- le misure di sicurezza tecniche e organizzative adottate.

Qualora il Titolare fosse individuato anche quale Responsabile esterno del trattamento, ai sensi dell'art. 28 del GDPR, dovrà redigere altresì il registro del Responsabile, contenente le seguenti informazioni:

- il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento;
- il nome e i dati di contatto di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento;
- il nome e i dati di contatto del RPD;
- le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
- una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto;

- nominare il RPD;
- nominare quale Responsabile del trattamento, ai sensi dell'articolo 28 GDPR, i soggetti pubblici o privati affidatari di attività e servizi per conto del Titolare stesso;
- nominare i Responsabili interni del trattamento.

Il Titolare, inoltre, favorisce l'adesione ai codici di condotta elaborati dalle Associazioni e dagli Organismi rappresentativi di categoria, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione della normativa europea e per dimostrarne il concreto rispetto da parte dell'Ateneo.

### 5.1.2. Contitolarità

Ai sensi di quanto disposto dal GDPR, è possibile che più soggetti condividano la titolarità al trattamento dei dati, qualora insieme definiscano finalità e mezzi del trattamento nonché provvedano congiuntamente ad adottare le misure di protezione adeguate.

La contitolarità può essere attuata e definita attraverso un contratto o una convenzione, definendo nello schema negoziale le reciproche responsabilità e dandone chiara e trasparente informazione ai cittadini (così come normato agli art.13 e 14 GDPR).

## 5.2 Responsabile della Protezione dei dati (RPD)

Il GDPR introduce, all'art. 37, una nuova figura, reclutata in funzione delle sue qualità professionali. Tra queste, in particolare, rilevano la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché la capacità di assolvere ai compiti assegnati.

Il RPD può essere un dipendente del Titolare del trattamento o assolvere i suoi compiti in base a un contratto di servizi.

Il RPD dell'Università di Milano – Bicocca è stato nominato con delibera del Consiglio di Amministrazione in data 24/04/2018, n. 228/2018/CDA, con decorrenza dal 15/05/2018. La nomina è stata comunicata al Garante in data 21.05.2018.
Per lo svolgimento dei propri compiti il RPD si avvale della collaborazione del personale assegnato all'URP.
L'Università non rimuove o penalizza il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.
I dati di contatto del RPD sono pubblicati sui siti internet istituzionali nell'apposita sezione denominata "Protezione dei Dati Personali".

### 5.2.1. Compiti e Responsabilità

Il RPD svolge i seguenti compiti:

- informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati. In tal senso può indicare al Titolare del trattamento i settori funzionali i settori funzionali da sottoporre a verifiche interne in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali e a quali trattamenti dedicare maggiori risorse e attenzione in relazione al rischio riscontrato;
- vigilare sull'osservanza della normativa relativa alla protezione dei dati, ferme restando le responsabilità del Titolare del trattamento. Rientra nell'attività di sorveglianza la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in ragione della loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR;
- effettuare, se del caso, consultazioni relativamente a ogni altra questione riguardante il trattamento e la protezione dei dati purché sia assicurata l'assenza di conflitto di interesse. Il ruolo di RPD, infatti, non può essere ricoperto da chi determina le finalità o i mezzi del trattamento, ossia, tra gli altri, dal Responsabile del Servizio di Protezione e Prevenzione, dell'Anticorruzione e Trasparenza, dai Sistemi informativi e/o da qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il Titolare assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine il RPD deve:

- essere invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili/Direttori di Dipartimento e dei Centri che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- disporre tempestivamente di tutte le informazioni pertinenti le decisioni che impattano sul trattamento e sulla protezione dei dati, in modo da poter rendere una consulenza idonea;
- essere consultato tempestivamente qualora si verifichi una violazione dei dati o altro incidente che comporti un rischio per i diritti e le libertà degli Interessati.

Nello svolgimento dei compiti affidatigli, il RPD deve debitamente considerare i rischi inerenti ai trattamenti, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei medesimi. In tal senso quest'ultimo:

- procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandolo sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati;
- redige una relazione annuale dell'attività svolta.

Il RPD dispone di autonomia e risorse per svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente. Il Titolare deve, quindi, fornire al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali e ai trattamenti. In particolare deve essere assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili/Direttori di Dipartimento e dei Centri e degli altri Organi di natura amministrativa;
- supporto adeguato in termini di risorse finanziarie, infrastrutturali e personali;
- accesso garantito ai settori funzionali dell'Ente così da fornire loro supporto, informazioni e input essenziali.

Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati e non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare. Nel caso in cui il RPD rilevi, direttamente o a seguito di segnalazioni, decisioni o azioni incompatibili con il GDPR e/o con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare e al Responsabile del trattamento.

Il RPD si avvale, nello svolgimento dei suoi compiti, anche di personale tecnico specializzato afferente all'Area dei Sistemi Informativi.

### 5.3 Responsabile interno (Designato)

Essendo difficilmente attuabile l'ipotesi che il Titolare possa, in una realtà complessa, garantire da solo la corretta adozione delle misure di sicurezza previste, nonché adempiere agli obblighi in materia di protezione dei dati personali, l'Ateneo, secondo quanto disposto dal precedente punto 3, ha ritenuto opportuno individuare i Responsabili interni, soggetti appositamente designati sulla scorta del proprio assetto organizzativo, conformemente a quanto previsto dal Codice Privacy, D.Lgs. 196/2003, come innovato dal D.Lgs. 101/2018 all'art. 2 *quaterdecies*. Il Responsabile Interno coadiuva il Titolare nella definizione delle finalità, delle modalità di trattamento e dei mezzi atti a garantire l'osservanza della normativa europea sulla protezione dei dati personali.

Nell'ambito della realtà universitaria e nel rispetto dell'esistente struttura organizzativa, i Responsabili interni al trattamento sono stati individuati nelle seguenti figure: Responsabili delle UU.OO.RR – Dirigenti d'Area, Direttori di Dipartimento, Direttori dei Centri di Ricerca, Medico competente, Prorettori, Delegati del Rettore, Responsabile scientifico (qualora, nell'ambito della propria attività di ricerca tratti dati personali la cui titolarità è dell'Ateneo, gestendoli su server dell'Ateneo stesso), nonché tutte le altre figure a queste affini. Questi, ciascuno per la propria area di competenza, garantiscono, insieme al Titolare, l'osservanza della normativa europea in tema di protezione dei dati personali.

I Responsabili interni sono nominati dal Rettore, in qualità di Legale rappresentante del Titolare, con apposita nota in cui impartisce loro tutte le istruzioni atte a garantire e dimostrare che il trattamento dei dati sia effettuato conformemente al GDPR.

Il Responsabile interno deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto, sulla base delle istruzioni fornite dal Titolare, le idonee misure tecniche e organizzative adeguate, rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR. In relazione a quanto previsto dal suddetto GDPR, il Responsabile interno è tenuto a comunicare preventivamente al Titolare del trattamento e al RPD eventuali nuovi trattamenti, la cessazione di trattamenti in corso, l'acquisizione di nuove tecnologie che prevedano il trattamento dei dati personali e comunicare tempestivamente al RPD eventuali casi di violazione dei diritti della libertà delle persone fisiche.

### 5.4 Referente per la protezione dei dati personali

Il Responsabile interno individua all'interno della propria area di competenza un collaboratore a cui assegnare il ruolo di Referente per la protezione dei dati personali.

Tale figura ha il compito di supportare il Responsabile in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il RPD e con l'Ufficio del RPD per tutte le attività inerenti alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia.

Egli ha anche il ruolo di raccordo con l'Area/Centro/Dipartimento di riferimento, dovendo provvedere altresì a formare e informare il personale della propria struttura in materia di protezione dei dati e sulle comunicazioni del RPD.

In relazione ai Centri di Servizio dei Dipartimenti, il Referente è individuato nel Responsabile amministrativo del Centro di Servizio, o in un suo delegato.

Il Referente per la protezione dei dati personali viene nominato per iscritto dal Responsabile del trattamento che gli impartisce tutte le istruzioni necessarie allo svolgimento dei propri compiti e finalizzate al rispetto delle norme. In caso di cessazione o revoca dell'incarico, il Responsabile interno comunica all'ufficio di supporto del RPD il nuovo nominativo.

### 5.5 Autorizzato

Il Titolare individua gli Autorizzati al trattamento, intesi come persone fisiche autorizzate a compiere operazioni di trattamento dati.

Gli Autorizzati al trattamento dei dati all'interno dell'Ateneo sono tutti coloro che quotidianamente gestiscono i dati, su supporto sia cartaceo sia informatico (personale tecnico amministrativo, docenti, ricercatori, assegnisti, borsisti etc). Essi devono trattare i dati personali, ai quali hanno accesso,

attenendosi alle istruzioni del Titolare e del RPD, avendo cura della natura e finalità dei trattamenti svolti, delle tipologie di dati personali oggetto di trattamento e delle misure tecnico organizzative attuate per la corretta protezione dei dati personali.

Gli Autorizzati al trattamento, che di norma sono i soggetti afferenti alla struttura di riferimento di ogni Responsabile Interno, sono adeguatamente formati e ricevono al momento della designazione specifiche istruzioni dal Titolare. I soggetti che verranno assunti dopo la nomina dovranno anch'essi essere adeguatamente formati in materia di trattamento e protezione dei dati personali.

Nello specifico, l'Autorizzato è tenuto:

- a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante la stessa;
- a non comunicare senza legittima autorizzazione a terzi o comunque diffondere, con o senza l'ausilio di strumenti elettronici, notizie, informazioni o dati appresi, relativi a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di soggetto incaricato/autorizzato e per effetto delle attività svolte;
- a seguire i seminari d'informazione e formazione in materia di protezione dei dati personali, obbligatori alla luce delle nuove disposizioni del regolamento privacy europeo e a sostenere i relativi test conclusivi finalizzati alla verifica dell'apprendimento;
- a segnalare con tempestività al proprio responsabile di ufficio e al referente eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante Privacy e ai soggetti Interessati (violazione dei dati).

L'Autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici aziendali per ragioni estranee e comunque diverse rispetto a quello per il quale è stato abilitato per fini istituzionali e di servizio, può implicare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari ed esporre l'amministrazione a danni reputazionali.

Il soggetto autorizzato si impegna a osservare le istruzioni, le politiche in materia di sicurezza informatica e logica adottate dall'Ateneo.

Nel caso in cui non ricorrano le condizioni di cui al presente articolo, i dipendenti che, nello svolgimento dei propri compiti, vengono a conoscenza di dati personali, sono considerati come soggetti terzi rispetto all'amministrazione stessa, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.

Sono altresì autorizzati al trattamento, e per tali motivi devono essere adeguatamente formati e informati in materia, gli studenti che, in ragione dell'appartenenza ad un corso di studio e nello svolgimento dello stesso, si trovano, a titolo esemplificativo e non esaustivo, a:

- effettuare stage e tirocini in Enti terzi;
- effettuare ricerche per la redazione della tesi di laurea e/o altri elaborati sottoposti a valutazione didattica;
- partecipare ad attività relative ai corsi di specializzazione dell'Area Medica, tra cui, a titolo esemplificativo, l'attività in corsia presso strutture ospedaliere convenzionate con l'Ateneo;
- agire in relazione ad attività funzionalmente e sostanzialmente connesse con l'attività didattica e formativa dell'Ateneo.

In particolare, al fine informare lo studente, sarà allo stesso fornito il Manuale Operativo degli Autorizzati al trattamento, ove potrà reperire tutte le informazioni su come agire nel rispetto della normativa vigente.
Lo studente dovrà inoltre avere cura di somministrare agli Interessati l'informativa per la raccolta dei dati, utilizzando il modello approntato dal RPD e dall'Ufficio di Supporto – URP, compilato sulla scorta delle particolarità e dei riferimenti della ricerca da effettuare ai fini della redazione della tesi.
In ogni caso, al fine di poter provare che il tesista abbia adempiuto agli obblighi di informazione e raccolta del consenso, al momento del deposito del titolo della tesi dovrà consegnare agli uffici amministrativi a corredo della documentazione anche il modello di informativa utilizzato ed eventualmente i consensi raccolti se necessari.
Sono altresì da considerare autorizzati al trattamento i tirocinanti, gli stagisti, gli studenti collaboratori 150 ore e le figure a questi affini, che, in ragione del loro *status*, svolgono la propria attività all'interno dell'Ateneo. È pertanto onere dell'Ateneo formare e autorizzare il soggetto al trattamento dati in ragione dell'incarico o dell'attività che questi andrà a svolgere.
Qualora, invece, lo studente ricopra il ruolo di collaboratore, tirocinante o stagista in un Ente terzo, in ragione di una convenzione tra questo e l'Ateneo, sarà l'Ente ospitante a dover formare e autorizzare lo studente al trattamento dei dati nella propria struttura. Tale aspetto dovrà essere concordato con l'Ente al momento della stipula della convenzione unitamente alla qualifica che si intende attribuire allo studente ospitato dall'Ente terzo.

### 5.6 Amministratori di sistema

Sono i soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati o di sue componenti; sono anch'essi degli Autorizzati al trattamento e sono appositamente nominati.
Il Provvedimento del Garante Privacy del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) considera diverse figure come Amministratori di Sistema, tra i quali: gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza, e gli amministratori di sistemi software complessi; questi sono ruoli che vanno debitamente nominati e periodicamente verificati.
Stanti le peculiarità tecniche, l'Amministratore di Sistema ricopre un ruolo estremamente delicato: progetta, sviluppa e gestisce l'infrastruttura di rete, i server, i software ed i servizi applicativi di base occupandosi spesso della sicurezza e della protezione dei dati e delle risorse. Inoltre fornisce supporto tecnico (help desk) e informatico su software e hardware. Quando necessario, ricopre un ruolo proattivo nell'ambito delle notificazioni di violazioni di sicurezza dei dati, notificando al RPD eventuali anomalie riscontrate, malfunzionamenti o rischi di sicurezza.
Egli risponde, inoltre, delle attività svolte e delle conseguenze derivanti da un malfunzionamento della rete e supporta Responsabili del Trattamento e Autorizzati per gli aspetti di tipo tecnico informatico nelle normali attività operative.

### 5.7 Responsabile Esterno del Trattamento

Il Titolare può avvalersi, per il trattamento di dati, di soggetti pubblici o privati che, in qualità di Responsabili del trattamento, ai sensi del par. 1 dell'art. 28 del GDPR, forniscano le garanzie ivi previste. La nomina viene fatta per iscritto ed è condizionata, nella durata e nei contenuti,

dall'esistenza del contratto o altro atto giuridico in essere. Il trattamento è consentito e limitato al solo fine di dare attuazione agli adempimenti. Al termine del contratto, infatti, o nell'ipotesi di scioglimento, per qualsivoglia causa, del medesimo, la nomina di Responsabile decadrà automaticamente e i dati trattati dovranno essere resi ed eliminati dal proprio sistema informativo, dandone conferma all'Università anche attraverso la redazione di un verbale di distruzione.
Con riferimento all'obbligo di restituzione dei dati, il Responsabile esterno si obbliga, altresì, a utilizzare formati standard o da concordare a tal fine con il Titolare.
Il Responsabile esterno tratta i dati conformemente al GDPR, e si impegna a:

- non comunicare, diffondere, trasferire i dati a soggetti terzi né a Paesi terzi senza l'autorizzazione del Titolare e, in ogni caso, in conformità con le disposizioni del GDPR;
- verificare liceità e correttezza dei trattamenti effettuati ai sensi dell'art. 6 del suddetto Regolamento, l'osservanza di ogni disposizione in materia di protezione dei dati personali e rendere disponibili al Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge in materia, consentendo eventuali controlli dello stesso Titolare come disposto dall'art 28 par. 3 lett. h) del GDPR;
- adottare tutte le misure tecniche ed organizzative ai sensi dell'art. 32 del GDPR in tema di sicurezza;
- garantire che i soggetti da lui autorizzati al trattamento dati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- non utilizzare i dati trattati per finalità che non siano strettamente inerenti alla propria attività istituzionale;
- redigere il registro delle attività dei trattamenti nei modi e nei contenuti previsti dall'art. 30 del GDPR;
- eseguire la valutazione di impatto sulla protezione dei dati, di cui all'art. 35 del GDPR sopra citato;
- collaborare con il Titolare per l'attuazione delle prescrizioni impartite dal Garante;
- comunicare tempestivamente al Titolare qualsiasi situazione che possa configurare una violazione dei dati, ai sensi dell'art. 33 del GDPR;
- predisporre l'informativa di cui agli artt. 13 e 14 del GDPR, con verifica che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli Interessati;
- rilasciare all'Ateneo una dichiarazione ai sensi degli artt. 46 e 47 del DPR 445/2000, che i servizi/la fornitura dei beni oggetti del contratto in essere rispondono ai principi della protezione "dalla progettazione" ("*by design*") e "per impostazione predefinita" ("*by default*") di cui all'art. 25 del GDPR.

Il Responsabile può avvalersi di un altro Responsabile del trattamento (sub-responsabile) esclusivamente previa autorizzazione dell'Ateneo. Il Responsabile, qualora possibile, dovrà aderire ai codici di condotta o alle certificazioni di cui agli artt. 40 e 42 del GDPR.
Il Responsabile del trattamento deve garantire che chiunque agisca sotto la sua autorità e abbia accesso a dati personali, sia in possesso di adeguata formazione e istruzione e si sia impegnato alla riservatezza o sia vincolato da un idoneo obbligo legale di riservatezza e provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare.

### 5.8 Responsabile Scientifico

Sono i titolari di ricerche, nell'ambito di progetti nazionali e internazionali, e figure assimilate. Trattano i dati nell'ambito del proprio progetto di ricerca e sono i referenti per l'attività svolta. Nello specifico la titolarità al trattamento dei dati è così declinata:

- il Responsabile Scientifico è direttamente ed esclusivamente Titolare qualora svolga attività di ricerca riguardante, a titolo esemplificativo e non esaustivo, un GRANT individuale, un'attività finalizzata alla pubblicazione scientifica *et cetera.* Per tali motivi definisce finalità, mezzi e misure di sicurezza e tratta i dati in maniera autonoma, anche su server di cui ha titolarità esclusiva;

- il Responsabile Scientifico è Responsabile Interno (Autorizzato di I livello) qualora svolga attività di ricerca propria dell'Università di Milano - Bicocca, anche nell'ambito di attività di ricerca nazionali e internazionali. Per tali motivi è il Titolare (ossia in questo caso l'Ateneo) che definisce finalità, mezzi e misure di sicurezza, e i dati trattati dal Responsabile Scientifico sono conservati su server di proprietà dell'Ateneo. Questi, dunque, agisce in nome e per conto del Titolare e vigila sul trattamento e la protezione dei dati.

## 6. Responsabilizzazione (Accountability) e Formazione

L'Ateneo promuove ogni strumento di sensibilizzazione che possa consolidare una mentalità più attenta al pieno rispetto della riservatezza, alla corretta gestione del trattamento dei dati e al miglioramento della qualità del servizio offerto al cittadino/utente.
In ottemperanza all'art. 39 par. 1. lett. a) del GDPR, l'Università di Milano-Bicocca ha avviato un percorso formativo rivolto, in primis, al personale tecnico – amministrativo dell'URP che supporta il RPD in tutte le attività di coordinamento e supervisione in materia di protezione dei dati, e, successivamente, ai Responsabili interni e ai Referenti per la protezione dei dati personali, al fine di condividere e diffondere i criteri per una corretta applicazione della normativa. Per garantire, inoltre, la conoscenza capillare delle disposizioni del GDPR e l'ambito di trattamento dei dati personali, al momento dell'ingresso in servizio è fornita a ogni dipendente una specifica informativa, contenente tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale.
È stato poi organizzato un corso e-learning, fruibile sulla piattaforma online dell'Ateneo, rivolto a tutto il personale dell'Università. Il corso si compone di moduli suddivisi per argomento, che comprendono materiale informativo, spiegazioni e un test di valutazione alla fine di ogni modulo. A completamento del corso è rilasciato un attestato di partecipazione e superamento del corso stesso.
Sarà cura dell'Ufficio di supporto al RPD provvedere periodicamente alla revisione del materiale formativo, informativo e della modulistica pubblicati nell'apposita sezione "Protezione dei Dati Personali" del sito internet dell'Ateneo, anche adeguando i riferimenti legislativi nel caso di aggiornamenti della normativa. Nello specifico i modelli redatti e pubblicati sulla pagina dedicata del sito istituzionale comprendono i requisiti minimi essenziali richiesti dalla normativa vigente e sono adattabili alle specifiche esigenze di ogni caso concreto.

## 7. Presupposti di liceità del trattamento

I trattamenti sono effettuati dall'Ateneo sulla base dei seguenti presupposti di liceità, ai sensi dell'art. 6 del GDPR:

- prestazione del consenso da parte dell'Interessato;
- esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
- adempimento di un obbligo legale al quale è soggetto l'ente;
- esecuzione di un contratto con soggetti Interessati, o esecuzione di obblighi precontrattuali adottati su richiesta degli stessi;
- necessità di salvaguardare gli interessi vitali dell'Interessato o della collettività.

## 8. Trattamento dei dati

Ai sensi del par. 2 dell'art. 4 del GDPR, con il termine "trattamento", si intende: "*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*".
Ai sensi dell'art. 5 del GDPR, presso l'Ateneo, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato (*principio di liceità, correttezza e trasparenza*);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia compatibile 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 (*limitazione della finalità*);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (*minimizzazione dei dati*);
d) esatti e, se necessario, aggiornati, pertanto sono adottate a tal fine le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati (*esattezza*);
e) conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: i dati personali 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR (*limitazione della conservazione*);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante idonee misure tecniche e organizzative, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (*integrità e riservatezza*);

g) trattati nel rispetto di tutti i principi citati essendo il Titolare responsabile che ciò avvenga e possa essere comprovato *(responsabilizzazione)*.

### 8.1 Applicativi con abilitazioni non selettive

Con riferimento agli applicativi con abilitazioni non selettive, tra i quali ad esempio Pentaho, che potrebbero comportare un accesso/utilizzo dei dati eccedenti le attività strettamente connesse alla finalità dei trattamenti previsti e autorizzati, l'accesso avverrà con:

- limitazioni ai diritti di visibilità dei dati stessi, in ragione della singola finalità di trattamento, o
- previa sottoscrizione di un impegno di riservatezza, da sottoporre a tutti coloro che, a qualunque titolo, accedano all'applicativo, anche attraverso la previsione di una casella bloccante da spuntare per proseguire con l'accesso.

Da un primo censimento risulterebbe che le categorie di soggetti che vi accedono siano:

- studenti, solo se nominati negli Organi dell'Ateneo e nel PQA - Presidio della Qualità di Ateneo,
- personale tecnico amministrativo,
- docenti solo se specificamente autorizzati.

Tutti i soggetti di cui sopra dovranno essere adeguatamente formati al fine di poter trattare i dati nel rispetto del GDPR anche fornendo loro specifiche istruzioni.

Allo scopo di evitare un utilizzo/trattamento di dati eccedenti le finalità dei trattamenti previsti e autorizzati, è opportuno che quanti sono in possesso di specifiche autorizzazioni/credenziali per accedere a banche dati contenenti dati personali, accedano alle stesse autonomamente/direttamente, ossia senza servirsi di intermediari di sorta e sempre e solo per la finalità di trattamento dichiarata, autorizzata e correlata alla propria attività.

Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'Interessato, in conformità al presente Regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite anche in tal modo. Qualora possano essere conseguite attraverso un trattamento ulteriore, che non consenta o non consenta più di identificare l'Interessato, tali finalità devono essere conseguite in tal modo.

Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, o di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti quali l'accesso dell'Interessato, la rettifica, la limitazione, la cancellazione e l'opposizione, fatte salve le condizioni e garanzie di cui al paragrafo precedente, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento le citate finalità specifiche e tali deroghe sono necessarie al conseguimento delle stesse.

## 9. Sicurezza del trattamento

Ai sensi dell'art. 32 del GDPR il Titolare ha l'obbligo di mettere in atto tutte le misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato

dell'arte e dei costi di attuazione, nonché della natura del campo di applicazione, del contesto e delle finalità del trattamento, come anche dalla probabilità e gravità di possibili rischi per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento sono, tra le altre, la minimizzazione e la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali nonché la capacità di ripristinare tempestivamente l'accesso e la disponibilità dei dati in caso di incidente fisico o tecnico.

L'Ateneo ha adottato le seguenti misure tecnico-organizzative:

- sistemi di autenticazione: il trattamento di dati personali con strumenti elettronici è consentito esclusivamente al personale autorizzato e dotato di credenziali che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento, o a un insieme di specifici trattamenti. Le credenziali di autenticazione consistono in un codice identificativo associato a una password, composta da almeno otto caratteri o comunque da un numero di caratteri pari al massimo consentito. La password non deve contenere riferimenti agevolmente riconducibili all'operatore e deve essere modificata, oltre che al primo accesso, successivamente, almeno ogni 3/6 mesi a seconda delle tipologie di dati trattati. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- sistemi di autorizzazione: i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento previste. Periodicamente viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
- sistemi di protezione (antivirus; firewall; antintrusione; anti-malware; anti-spam);
- misure antincendio;
- sistemi di rilevazione di intrusione;
- sistemi di videosorveglianza;
- registrazione degli accessi;
- cartelli relativi agli accessi non autorizzati;
- porte, armadi e contenitori dotati di serrature e/o ignifughi;
- sistemi di backup e conservazione degli archivi elettronici;
- aggiornamento puntuale dei Sistemi Operativi dei server e delle PDL con le ultime patch;
- sistemi di webfiltering;
- sistemi di syslog.

La conformità del trattamento dei dati al GDPR è dimostrata, pertanto, attraverso l'adozione delle misure di sicurezza, l'adesione a codici di condotta approvati e/o a un meccanismo di certificazione approvato.

## 10. Comunicazione e pubblicazione dei dati

Le richieste volte ad ottenere la comunicazione di dati dovranno essere formulate per iscritto al Responsabile competente, il RPD, il Responsabile interno o il Titolare.
La comunicazione di dati a soggetti pubblici è sempre ammessa per i fini istituzionali.
Le richieste provenienti da soggetti privati ed enti pubblici economici possono essere accolte soltanto se previste da norme di legge o di regolamento.
Le richieste devono essere adeguatamente motivate e devono contenere:

- il nome, la denominazione o la ragione sociale del richiedente;
- i dati richiesti, le finalità e le modalità di utilizzo degli stessi.

Al fine di agevolare l'inserimento nell'ambito lavorativo e professionale degli studenti e dei laureati dell'Ateneo, l'Università, se in possesso del relativo consenso degli Interessati, può effettuare la comunicazione dei loro dati a enti privati e consorzi interuniversitari che ne facciano la richiesta.
L'Ateneo potrà stabilire le modalità di comunicazione dei predetti dati, per la quale può essere richiesto un contributo a copertura dei costi sostenuti.
L'Università ha la facoltà di inviare ai propri studenti e laureati, anche tramite soggetti esterni, materiale informativo relativo a ulteriori propri percorsi formativi.
L'Ateneo, in ragione di quanto disposto dalla normativa vigente in materia di trasparenza, ha obblighi in ordine alle pubblicazioni di talune categorie di atti.
Verificata la sussistenza dell'obbligo di pubblicazione dell'atto o del documento nel proprio sito web istituzionale, l'Ateneo deve limitarsi a includere negli atti da pubblicare solo quei dati personali realmente necessari e proporzionati alla finalità di trasparenza perseguita nel caso concreto.
Pertanto, prima di procedere alla pubblicazione sul proprio sito, l'Ateneo deve effettuare i seguenti passaggi:
- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;
- verificare, caso per caso, se ricorrano i presupposti per l'oscuramento di determinate informazioni;
- sottrarre all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari, come ricordati al punto precedente.

In ogni caso è vietato diffondere dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.
Dati ulteriori rispetto a quelli per i quali è prevista la pubblicazione obbligatoria, questi potranno essere oggetto di pubblicazione, a patto che questi vengano resi effettivamente anonimi e non vi sia più la possibilità di identificare gli interessati, nemmeno indirettamente e in un momento successivo.
Pertanto, nella pubblicazione dei provvedimenti, si dovrà provvedere a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.
Con riferimento ai dati contenuti nei provvedimenti/atti da pubblicare, dovranno essere rispettate le seguenti indicazioni di massima:

- nei provvedimenti di conferimento incarico, il nome e cognome del dipendente/docente può comparire per esteso, senza altri dati non strettamente funzionali all'ottemperanza degli obblighi di legge.
- Nelle graduatorie di concorsi relativi ai docenti, al PTA e agli studenti, nonché negli elenchi con esiti di prove e/o esami di profitto, graduatorie *et similia,* occorre inserire il nome e il cognome e la data di nascita; ove il software lo consentisse, la data di nascita dovrà essere inserita solo in caso di omonimia e in nessun caso andrà indicato il codice fiscale.
- Nei provvedimenti in cui vi è anche indirettamente la possibilità di rivelare informazioni sullo stato di salute, l'origine nazionale e/o altre categorie particolari di dati, occorrerà oscurare il nome o indicare l'iniziale del nome e il cognome.
- Nei documenti analogici digitalizzati oscurare la firma autografa del soggetto che ha sottoscritto il documento.

## 11. Sanzioni

Il trattamento illecito dei dati o la loro perdita determina in capo al Titolare:
una responsabilità di natura penale per la mancata adozione di misure minime di sicurezza;

- una responsabilità di natura civile in quanto l'omissione di misure idonee determina un obbligo risarcitorio ai sensi dell'art. 2050 del Codice Civile e ai sensi dell'art.15 del D.Lgs.196/03;
- una responsabilità di tipo amministrativo.

In merito a quest'ultima, il GDPR, all'art.83, prevede sanzioni amministrative pecuniarie fino a 10 milioni di euro e, per le imprese, pari al 2% del fatturato di gruppo mondiale, in caso di violazione degli obblighi del Titolare del trattamento (artt. 8,11 da 25 a 39, 42, 43) e fino a 20 milioni di euro e, per le imprese, pari al 4% del fatturato di gruppo mondiale, in caso di violazione delle condizioni relative al consenso (artt. 5,6,7,9), al rispetto dei diritti dell'Interessato (artt. da 12 a 22) e dei trasferimenti dati da un Titolare ad un altro in Paesi terzi (artt. da 44 a 49).
Ai sensi di quanto disposto dall'art. 2 *decies* del D.Lgs. 196/2003, i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall'articolo 160 *bis*, relativamente ai procedimenti giudiziari.

## 12. Responsabilità

Chiunque subisca un danno materiale o immateriale a seguito della violazione del presente Regolamento ha il diritto di ottenerne il risarcimento dal Titolare del trattamento o dal Responsabile esterno del trattamento; in quest'ultimo caso il Responsabile esterno risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente Regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.
Il Titolare e il Responsabile esterno del trattamento sono esonerati dalla responsabilità, a norma del paragrafo 2 dell'articolo 82 del GDPR se dimostrano che l'evento dannoso non gli è in alcun modo imputabile.

Qualora più Titolari o Responsabili del trattamento, anche congiuntamente, siano coinvolti nello stesso trattamento e risultino, ai sensi dei paragrafi 2 e 3 dell'articolo 82 GDPR, responsabili del danno causato dal trattamento, ciascun Titolare o Responsabile del trattamento è ritenuto responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'Interessato. Qualora un Titolare o un Responsabile del trattamento abbia corrisposto, conformemente al paragrafo 4 dell'articolo 83 del GDPR, l'intero risarcimento del danno, questi avrà il diritto di reclamare dagli altri Titolari o Responsabili del trattamento, coobbligati e coinvolti nello stesso trattamento, la quota del risarcimento corrispondente alla loro parte di responsabilità per il danno causato, conformemente alle condizioni di cui al paragrafo 2, articolo 83, del GDPR.
Le azioni legali per l'esercizio del diritto ad ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2 del GDPR

## 13. Dati trattati

Nell'esercizio delle proprie funzioni istituzionali l'Ateneo tratta le seguenti categorie di dati:

- "Dati personali": qualsiasi informazione riguardante una persona fisica identificata o identificabile («Interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- "Categorie particolari di dati": i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale;
- "Dati genetici": 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;
- "Dati biometrici": dati personali ottenuti da un trattamento tecnico 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;
- "Dati relativi alla salute": 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;
- "Dati giudiziari": dato personale idoneo a rivelare i provvedimenti giudiziari penali, civili e amministrativi.

L'Ateneo tratta i dati biometrici, genetici, relativi alla salute e giudiziari anche sulla base di quanto specificatamente previsto dagli artt. 2 *septies* e 2 *octies* del D.Lgs. 196/2003, come novellato dal D.Lgs. 101/2018.

L'Ateneo tratta con misure adeguate le seguenti tipologie di dati, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto, delle finalità del trattamento:
a) dati, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, ivi compresi i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nell'Università. A titolo esemplificativo e non esaustivo ci si riferisce a dati inerenti a:

- 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 la sicurezza delle persone nei luoghi di lavoro;
- erogazione del servizio di telefonia fissa e mobile.

b) Dati relativi a "studenti" intesi nell'accezione più ampia, e per tutte le attività e modalità connesse alla qualità di "studente" e ai laureati. A titolo esemplificativo e non esaustivo ci si riferisce a dati inerenti a:

- attività di orientamento;
- erogazione dei test di ingresso o alla verifica dei requisiti di accesso;
- erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea);
- attività di tirocinio;
- attività di job placement;
- 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;
- servizi di tutorato, assistenza, inclusione sociale;
- servizi e attività per il diritto allo studio;
- procedimenti di natura disciplinare 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, conto terzi e/o connessi ad attività trasversali. A titolo esemplificativo e non esaustivo ci si riferisce a dati inerenti a:
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;
- erogazione federata di servizi;

- erogazione del servizio Eduroam;
- accesso a servizi federati;
- accesso ai servizi con autenticazione SPID;
- tracciamento di informazioni non primarie.

## 14. Registro dei trattamenti

Ai sensi dell'art. 30 del GDPR, *"Ogni Titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità"*.

La costituzione, la tenuta e l'aggiornamento del Registro delle attività di trattamento sono, dunque, obblighi gravanti sul Titolare.

Tale documento ha una doppia valenza: la prima di tipo operativo e funzionale alla gestione organica e sistematica dei dati trattati, la seconda di tipo probatorio ex post, quale documento da esibire in caso di audit da parte dell'Autorità Garante, al fine di dimostrare - nell'ottica del principio di responsabilizzazione - la conformità al GDPR.

La mancata tenuta del registro delle attività di trattamento può essere soggetta alla sanzione amministrativa pecuniaria fino a 10 milioni di euro.

La costruzione sistematica del registro, la sua tenuta ed il suo aggiornamento possono essere effettuate in forma scritta, anche in formato elettronico.

Al fine di redigere le schede, una per ogni singola finalità del trattamento effettuato da ciascuna singola Area, Dipartimento o Centro dell'Ateneo, occorre censire le singole attività correlate ai diversi processi.

Tale operazione è effettuata mediante una primaria attività di ricognizione di tutte le informazioni connesse ai trattamenti dei dati all'interno dell'Ateneo. Le informazioni necessarie sono reperite attraverso:

- la mappatura dei processi dell'Ateneo in cui sono riportate le attività di trattamento;
- la ricognizione delle schede dei trattamenti precompilate;
- la valutazione puntuale dei trattamenti e dei flussi di dati interni ed esterni;
- il confronto, tramite colloqui e interviste, con i Referenti ed i collaboratori delle diverse unità organizzative che gestiscono tali processi.

L'aggiornamento del Registro avviene con regolarità a cadenze prestabilite, costituendo un preciso onere del Titolare che le schede siano una rappresentazione realistica e dinamica dei trattamenti posti in essere dall'Ateneo.

In particolar modo, sarà necessario provvedere ad un aggiornamento del Registro in presenza di ogni cambiamento organizzativo, operativo e tecnologico rilevante e tale da impattare sulla gestione dei dati personali.

A tal fine, è stato istituito il flusso informativo periodico verso tutti i Referenti; in particolare, nelle more dell'implementazione del software acquistato per l'aggiornamento su data base delle schede di trattamento, l'aggiornamento delle schede già censite il 25 maggio 2018, redatte in file word e pdf, avverrà con cadenza regolare, di norma annuale, su impulso del RPD, tranne nel caso in cui vi sia necessità e sia richiesta da un Referente per la protezione dati.

Alla ricezione della e-mail con la richiesta di aggiornamento, il Referente di ogni singola Area, Dipartimento o Centro, dovrà aggiornare le schede di propria competenza, aggiungendo eventuali nuove finalità ed espungendo quelle che non dovessero più rientrare fra le attività svolte; tali schede dovranno poi essere inviate tramite e-mail al RPD per l'inserimento nel Registro, che dovrà essere validato dal Titolare.
Una volta che il software verrà implementato, a seguito di una necessaria e adeguata formazione, ciascun Referente aggiornerà la scheda nel programma alle cadenze prestabilite senza necessità di inviare il file al RPD tramite e-mail.

## 15. Valutazione d'impatto

L'Università, quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della natura, dell'oggetto, del contesto, delle finalità del trattamento e dell'utilizzo di nuove tecnologie, effettua, ai sensi dell'art. 35 del GDPR, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano analoghi rischi elevati.
L'Ateneo svolge la valutazione d'impatto sulla protezione dei dati con il RPD.
La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

a) una 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 analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR, o di dati relativi a condanne penali e a reati;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'Università si consulta con il RPD anche per assumere la decisione di effettuare o meno la valutazione d'impatto; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della valutazione di impatto qualora effettuata. Il Titolare può, documentandone le motivazioni, adottare condotte difformi da quelle raccomandate dal RPD.
I Referenti per la protezione dei dati devono collaborare nella conduzione della valutazione di impatto fornendo ogni informazione e documentazione necessaria.
Il Responsabile per la transizione al digitale fornisce supporto ai Referenti e al RPD per lo svolgimento della valutazione di impatto e pubblica le relative linee guida in materia.
L'Università consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato.
L'Università consulta il Garante per la Protezione dei dati personali anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

## 16. Informativa

In ottemperanza ai disposti degli artt. 13 e 14 del GDPR, l'Università ha provveduto a rivedere tutte le informative presenti, pubblicate sul sito istituzionale.

Ogni UOR, Dipartimento e Centro di ricerca predispone la propria informativa, riferita alle finalità connesse alle attività di competenza. Nello specifico ogni struttura ha la facoltà di redigere una informativa generale, comprendente tutte le finalità, o tante informative singole quante sono le finalità.

L'informativa è fornita verbalmente, per iscritto attraverso consegna a mano della stessa, attraverso la pubblicazione sulle pagine di ciascuna UOR del sito web di Ateneo e sui siti web di ciascun Dipartimento e Centro di Ricerca, nonché tramite affissione nei locali dell'Ateneo dove vi sia ricevimento del pubblico e front office.

I modelli di informativa, e, in generale, tutta la modulistica riferita alla protezione dei dati è pubblicata sul sito internet istituzionale nella apposita sezione denominata "Protezione dei Dati Personali".

L'informativa contiene:

- l'identità e i dati di contatto del Titolare del trattamento;
- i dati di contatto del RPD;
- le finalità e le modalità del trattamento cui sono destinati i dati personali;
- esistenza o meno di un processo decisionale automatizzato;
- trasferimento o meno di dati a paesi terzi e/o organizzazioni internazionali;
- i destinatari dei dati;
- il periodo di conservazione dei dati;
- la base giuridica del trattamento;
- i diritti dell'Interessato.

## 17. Consenso

Ai sensi dell'art. 6 par. 1, lett. c), d), e), del GDPR, l'Ateneo non è tenuto a richiedere il consenso al trattamento dei dati personali per tutte quelle finalità inerenti alle attività istituzionali dell'Università, ove necessarie per ottemperare ad obblighi di legge e per ragioni di pubblica sicurezza.

Per tutte le finalità che non rientrano nelle attività istituzionali, o per le quali il trattamento sia reso obbligatorio da previsioni di legge o da ragioni di pubblica sicurezza, dovrà essere richiesto il consenso; il consenso verrà raccolto tramite sottoscrizione del modulo cartaceo fornito in calce all'informativa relativa al trattamento in oggetto o tramite spunta delle caselle ove sia richiesto in procedure online, quali i form di iscrizione sul sito istituzionale, o con sottoscrizione digitale del modulo.

Con riferimento al consenso al trattamento dei dati da parte degli studenti, questo non è necessario, essendo il trattamento effettuato per una attività sotto copertura normativa.

In merito alla attività di ricerca, il consenso al trattamento dei dati non è dovuto qualora la ricerca sia svolta sotto l'egida dell'Ateneo, e che dunque quest'ultimo ne sia il Titolare. Qualora invece si tratti di un GRANT individuale, per il quale il Titolare è individuato nel Responsabile scientifico, in quel caso occorrerà raccogliere il consenso.

Il consenso è obbligatorio nel caso in cui l'attività didattica, di ricerca o amministrativa comportino il trattamento di dati di soggetti minori di 16 anni. In quel caso, invero, occorrerà richiedere il consenso a entrambi i genitori o a chi esercita la responsabilità genitoriale.

Il consenso al trattamento dei dati non deve essere confuso con il "consenso informato", che non è disciplinato nel presente Regolamento, necessario per poter sottoporre un paziente ad un determinato trattamento sanitario, anche nell'ambito della ricerca.
L'acquisizione dei consensi può avvenire sia analogicamente, con sottoscrizione autografa, sia digitalmente.
Qualora il consenso venga raccolto digitalmente, tale acquisizione avverrà con differenti metodi e soluzioni tecnologiche la cui individuazione, rispetto alla adattabilità ai propri processi, è lasciata alla discrezionalità della singola struttura, non esistendo al momento specifiche linee guida nazionali.
Tra i metodi più comuni e utilizzabili, nel contesto normativo italiano, per consentire all'utente di sottoscrivere digitalmente documenti informatici, si richiamano in maniera esemplificativa e necessariamente non esaustiva (essendo oggetto di eventuali aggiornamenti normativi):
- Firma elettronica semplice;
- Firma Elettronica Avanzata grafometrica anche di tipo biometrico (FEA - GFM);
- Firma Elettronica Avanzata - Carta Nazionale dei Servizi (FEA-CNS)/OTP etc;
- Firma digitale qualificata;
- Servizio Pubblico di Identità Digitale (SPID).

## 18. Diritti dell'Interessato

Il Titolare del trattamento deve adottare, tra le altre, le misure tecniche ed organizzative necessarie per favorire l'esercizio da parte degli Interessati dei propri diritti nonché, di conseguenza, il riscontro, che dovrà avere forma scritta (anche elettronica), alle istanze in tal senso da questi presentate.
Ai sensi dell'art 15 del GDPR, l'Interessato ha il diritto di chiedere al Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di:

- accedere ai propri dati personali;
- conoscere le finalità del trattamento e le categorie di dati personali in argomento;
- essere informato sugli eventuali destinatari dei dati personali;
- essere al corrente del periodo di conservazione dei dati;
- poter rettificare e/o cancellare i dati;
- limitare e/o opporsi al trattamento;
- poter proporre reclamo a un'Autorità di controllo.

I sopra elencati diritti, di cui agli articoli da 15 a 22 del GDPR, se riferiti ai dati personali di persone decedute, possono, a norma dell'art. 2 *terdecies* del D.Lgs. 196/2003, essere esercitati da chi ha in merito un legittimo interesse proprio, o da chi agisce a tutela dell'Interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
Relativamente al diritto dell'Interessato alla cancellazione dei propri dati, va specificato che non può essere applicato indiscriminatamente a tutti i documenti redatti/acquisiti/archiviati presso l'Ateneo in quanto il trattamento dei dati è necessario per motivi di interesse pubblico nel settore dell'Istruzione, come previsto dall'art. 17, par. 3 del GDPR.
Tenuto conto del fatto che l'archivio dell'Ateneo, essendo parte di un Ente pubblico, è sottoposto al controllo della Soprintendenza Archivistica e soggiace a particolari obblighi, limitazioni e procedure autorizzative, sono state pubblicate le Linee guida del Massimario per la selezione e lo scarto dei

documenti conservati nell'archivio stesso, ove sono esplicitati i criteri per la cancellazione/distruzione dei documenti, con l'indicazione altresì delle categorie di documenti che possono essere distrutti, i tempi di conservazioni e le procedure per la richiesta di cancellazione.
Il Titolare del trattamento deve fornire, se richiesto dall'Interessato, copia dei dati personali oggetto di trattamento, purché non vengano lesi i diritti e le libertà altrui. In caso di ulteriori copie richieste, il Titolare del trattamento addebita un contributo spese basato sui costi amministrativi indicati nelle procedure dell'Ateneo. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'Interessato stesso, le informazioni sono fornite in un formato elettronico di uso comune.
Il riscontro formale all'istanza deve pervenire all'Interessato entro 30 giorni dalla ricezione dell'istanza stessa, 90 giorni in casi di particolare complessità.
La struttura preposta alla gestione dell'istanza è l'Ufficio per le Relazioni con il Pubblico, individuato quale ufficio a supporto del Responsabile della Protezione Dati.
Il processo di gestione delle istanze viene gestito secondo le seguenti fasi:

1) perviene l'istanza via e-mail o PEC con utilizzo della apposita modulistica disponibile sulla pagina dedicata del sito d'Ateneo.
2) L'istanza viene registrata a protocollo dal Settore gestione documentale e viene classificata secondo il Sistema di gestione documentale:
   - se l'istanza è pervenuta a mezzo PEC, il Settore gestione documentale attribuisce la visibilità all'Ufficio URP nel Sistema di gestione documentale;
   - se l'istanza è pervenuta a mezzo e-mail, sarà cura dell'Ufficio URP richiedere la protocollazione dell'istanza.
3) Viene accertata l'identità dell'istante e la legittimazione dello stesso a presentare l'istanza:
   - in caso negativo, l'istanza viene dichiarata inammissibile con comunicazione all'istante;
   - in caso positivo, l'istanza viene dichiarata ammissibile.
4) Viene comunicata all'interessato la presa in carico dell'istanza ammissibile.
5) L'istanza ammissibile viene comunicata al Titolare.
6) Si procede all'istruttoria della pratica, secondo le seguenti fasi:
   6.1.) accertamento alla fonte in merito al soggetto detentore del dato, con interpello del Referente dell'Area/Dipartimento/Centro di riferimento e del Dirigente/Direttore del Dipartimento o del Centro, che deve dare riscontro entro 5 giorni;
   6.2.) accertamento relativo agli adempimenti da effettuarsi nei confronti dell'interessato, ed in particolare su somministrazione dell'informativa, modalità di trattamento del dato e modalità e destinazione di eventuali trasferimenti a terzi, da completarsi entro i successivi 5 giorni.
7) Viene redatto dall'Ufficio di supporto un documento costituente l'istruttoria dell'istanza, corredato dalle possibili risposte alla stessa, sottoscritto dal Responsabile della Protezione dei Dati e sottoposto al vaglio del Titolare;
8) Viene redatto dall'Ufficio di supporto il riscontro formale da inviare all'interessato in base a quanto disposto dal Titolare.
9) Il riscontro, sottoscritto dal Titolare, viene inoltrato dall'Ufficio di supporto all'interessato attraverso la medesima modalità di trasmissione dell'istanza, entro 30 giorni dal giorno in cui

è pervenuta. Nel caso di istanza di cancellazione, ove sia necessario eliminare un intero documento, il file contenente il dato deve essere sostituito con un altro, riportante la seguente dicitura "*Documento eliminato ai sensi dell'art. 17 GDPR*". Eventuali ritardi legati alla complessità del caso saranno comunque comunicati all'istante e debitamente motivati. La risposta deve essere definitiva non oltre i successivi 90 giorni. Nel periodo dal 22 dicembre al 2 gennaio e dal 10 al 20 agosto i termini sono sospesi.

Il Responsabile della Protezione dei Dati provvede annualmente a redigere un report relativo al numero e alla tipologia delle istanze pervenute nel rispetto del principio dell'*accountability*.

Il riscontro formale deve essere sottoscritto dal Titolare, protocollato e inviato all'Interessato.

I diritti di cui agli articoli da 15 a 22 del GDPR soggiacciono alle limitazioni previste dagli articoli 2 *undecies* e 2 *duodecies* del D.Lgs. 196/2003, tra cui si annoverano casi particolari di protezione dell'Interessato e casi di pubblico interesse concernente i procedimenti giudiziari.

## 19. Violazione dei dati

Per violazione dei dati personali, si intende qualsiasi evento, che si traduca in una la violazione di sicurezza, la quale comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ateneo.

I principali rischi per i diritti e le libertà degli Interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono di seguito indicati:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale.

Qualora il Titolare dovesse ritenere che il rischio per i diritti e le libertà degli Interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi (art. 34 del GDPR).

Il rischio per i diritti e le libertà degli Interessati può essere considerato:

- alto: quando la violazione può, a titolo esemplificativo, coinvolgere un rilevante quantitativo di dati personali e/o di soggetti Interessati, riguardare categorie particolari di dati personali, comprendere dati che possono accrescere ulteriormente i potenziali rischi (dati di localizzazione, finanziari, relativi alle abitudini e preferenze) e i rischi, imminenti e con un'elevata probabilità di accadimento, impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (persone fragili, minori, soggetti indagati ecc.);
- medio: quando gli Interessati potrebbero andare incontro a conseguenze superabili sebbene con una certa difficoltà, come, a titolo esemplificativo, danni non eccessivi alla proprietà, citazione in giudizio, limitato peggioramento della salute, ecc.;
- basso: quando gli Interessati potrebbero incontrare disagi, superabili con difficoltà limitate, come eventuali ritardi di accesso ai servizi d'Ateneo, stress, ecc.;

- trascurabile: nel caso in cui gli Interessati non sarebbero danneggiati o potrebbero incontrare solo inconvenienti non rilevanti.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli Interessati, deve provvedere, in ottemperanza all'art. 33 del GDPR, alla notifica al Garante per la protezione dei dati, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Chiunque (Responsabili interni, Referenti per la protezione dei dati e/o Autorizzati) venga a conoscenza di eventuali violazioni è tenuto ad informare tempestivamente il Titolare ed il RPD.

Il RPD ha provveduto a organizzare il flusso per la procedura di segnalazione di violazione di dati personali.

Se la violazione si verifica per trattamenti riguardanti attività svolte dalle Aree dell'Amministrazione Centrale, chi ne viene a conoscenza deve immediatamente segnalarla al Referente individuato nella struttura ovvero al Capo Area; se la violazione, invece, si verifica per trattamenti inerenti alle attività svolte dai Dipartimenti, chi ne viene a conoscenza deve immediatamente segnalarla al Referente individuato nel Dipartimento o al Direttore del Dipartimento stesso. Questi ultimi a loro volta entro le 24 ore successive alla segnalazione, dovranno trasmettere la notizia via e-mail al RPD, all'indirizzo rpd@unimib.it. La procedura, nonché la modulistica necessaria a segnalare l'avvenuta violazione, sono state esplicitate dal RPD durante gli incontri con i Referenti, i quali sono stati inoltre sensibilizzati in particolar modo sulla tempistica da rispettare. Si rimanda espressamente all'analisi della documentazione/modulistica pubblicata sulla pagina web "Protezione dei dati personali" del sito istituzionale.

A seguito della comunicazione di violazione dei dati, tramite invio dell'apposito modulo, il RPD richiede ai tecnici dell'Area Sistemi Informativi un report tecnico inerente la violazione, che deve pervenire entro e non oltre le 24 ore successive alla richiesta, debitamente sottoscritto dal Responsabile dell'Area o da un suo delegato; eventuali ritardi nella trasmissione del report dovranno essere adeguatamente motivati. Nel suddetto report devono essere specificati i seguenti elementi:

- la portata della violazione, con esposizione descrittiva delle fasi dell'attacco, la provenienza (se nota) dell'evento ed eventuali compromissioni;
- le procedure di mitigazione e/o di eliminazione dell'evento violativo apportate e/o da apportare ai sistemi informatici di Ateneo;
- l'impatto dell'evento sui sistemi, sulla rete e sulle postazioni d'Ateneo prima e dopo gli interventi di mitigazione e/o di eliminazione;
- conclusioni tecniche sull'intero evento.

Il RPD, con l'ausilio dell'URP, svolge l'istruttoria sulla violazione tenendo conto del report tecnico fornito, sulla base del quale propone al Titolare la segnalazione all'Autorità, qualora questo sia effettivamente da considerarsi un evento di violazione dei dati in base alla normativa vigente.

Il report tecnico dovrà essere corredato della cristallizzazione dei dati relativi all'attacco, ove questo costituisse una violazione di dati, allo scopo di poterli estrarre ai fini probatori, secondo i dettami dell'informatica forense (anche nota come *digital forensics*), per la necessaria denuncia querela alle autorità competenti.

Il Titolare, alla luce dell'istruttoria svolta dal RPD, adotta le misure necessarie e procede alla eventuale segnalazione della violazione al Garante.

Il Titolare deve opportunamente documentare tutte le violazioni di dati personali subite, anche se non comunicate alle Autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.
All'uopo è stato predisposto il registro degli incidenti informatici, ove sono ricomprese anche le violazioni di dati, su cui il Titolare, il RPD e l'Ufficio di supporto a quest'ultimo, annotano tutte le segnalazioni di incidenti informatici, anche se non trasmesse all'Autorità Garante.
Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

## 20. Videosorveglianza

Il Titolare, per il tramite dei Responsabili interni, ove siano in funzione strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio, assicura il rispetto degli standard individuati nel provvedimento generale del Garante del 10 aprile 2010 e ss.mm.ii., per la gestione del trattamento dei dati tramite apparecchiature per la videosorveglianza.

## 21. Disposizioni finali

Per tutto quanto non espressamente disciplinato nel presente Regolamento si applicano le disposizioni del GDPR e tutte le norme vigenti in materia, nonché i Regolamenti d'Ateneo purché non confliggenti.
In caso di conflitto tra le disposizioni del presente Regolamento con quelle del "Regolamento per il trattamento dei dati sensibili e giudiziari in attuazione del D.Lgs. 196/2003", Reg. di Ateneo n. 012891 del 23.12.2005, queste ultime si devono intendere disapplicate per il principio di successione.

## 22. Approvazione, emanazione ed entrata in vigore

Il presente Regolamento è approvato dal Consiglio di Amministrazione d'Ateneo ed è emanato con Decreto Rettorale.
Il Regolamento entrerà in vigore il giorno successivo alla sua pubblicazione sull'albo online d'Ateneo.

## 23. Revisione

Il presente Regolamento sarà aggiornato a seguito dell'emanazione di normativa sopravvenuta. Per l'approvazione, anche della revisione, si seguirà l'iter di cui all'art. 22.
L'aggiornamento o la modifica di uno o più allegati al Regolamento non comporta la revisione dell'intero Regolamento.

## 24. Allegati

Di seguito si allegano i modelli licenziati e consolidati alla data di approvazione del presente Regolamento. Gli aggiornamenti dei modelli, necessari per le eventuali sopravvenienze, saranno pubblicati sulla pagina "Protezione dei Dati Personali" sul sito istituzionale.

IL RETTORE

*Prof.ssa Maria Cristina Messa*

Visto il Direttore Generale

*Dott.ssa Loredana Monica Elisabetta Luzzi*

Visto il Responsabile della Protezione Dati

*Dott.ssa Maria Bramanti*