UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

UOR: Area Affari Istituzionali, Legali e Comunicazione - Settore Legale di supporto al RPD

Estensore: dott.ssa Emanuela Mazzotta

LA RETTRICE

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;

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

CONSIDERATA la necessità di revisionare, principalmente tramite un intervento di carattere redazionale, il "Regolamento per il trattamento e la protezione dei dati personali", pubblicato in Ateneo nel 2018 (prot. 90980/18 del 03/12/2018), pubblicato in sede di prima e generale applicazione della disciplina della protezione dati relativa alla comunità universitaria successivamente all'entrata in vigore del GDPR;

VALUTATA la necessità di accorpare i contenuti del Regolamento dei dati sensibili e giudiziari, pubblicato nel 2005, al nuovo testo del Regolamento interno in ossequio ai principi di semplificazione e razionalizzazione;

VISTA la delibera adottata dal Consiglio di Amministrazione in data 20 dicembre 2022, 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.

La Rettrice

Prof.ssa Giovanna Iannantuoni

(Firmato digitalmente ai sensi dell'art. 24 del D.Lgs. 82/05)

REGOLAMENTO PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI

INDICE

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

PARTE GENERALE

1. Oggetto, campo di applicazione e finalità

Il presente Regolamento, adottato in attuazione del GDPR e del D.Lgs. 196/2003 come novellato dal D. Lgs. 101/2018 ("Codice in materia di protezione dei dati personali"), disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi presso l'Università degli Studi di Milano Bicocca, con lo scopo di definire e individuare 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.
L'Ateneo effettua, con o senza l'ausilio di processi automatizzati, i trattamenti di dati per il raggiungimento dei propri fini istituzionali, con particolare riferimento alle attività di ricerca, didattica, terza missione e amministrazione, nonché agli ulteriori servizi o attività previsti in convenzioni e contratti stipulati dall'Ateneo con soggetti pubblici e privati, nel rispetto dei diritti, delle libertà fondamentali e della dignità dell'Interessato.

2. Definizioni

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

1. "GDPR": 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.
2. "Codice della Privacy": il D.Lgs. 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali" e ss.mm.ii.
3. "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;
4. "dato personale": qualunque informazione riguardante una persona fisica identificata 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;
5. "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;

6. "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;
7. "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;
8. "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;
9. "dati giudiziari": dato idoneo a rivelare i provvedimenti giudiziaria carico dell'interessato di natura penale, civile o amministrativa.
10. "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;
11. "Contitolare": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altro/i titolare/i del trattamento, determina le finalità e i mezzi del trattamento dei dati personali;
12. "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);
13. "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;
14. "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;
15. "Referenti per protezione dei dati": figure che hanno il compito di supportare il Responsabile Interno Designato 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;
16. "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);
17. "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);

18. "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;
19. "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;
20. "Interessato al trattamento": la persona fisica a cui si riferiscono i dati personali;
21. "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;
22. "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;
23. "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;
24. "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;
25. "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.
26. "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;
27. "limitazione di trattamento": il contrassegno dei dati personali, conservati con l'obiettivo di limitarne il trattamento in futuro;
28. "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;
29. "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;

30. “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;
31. “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;
32. “Autorità di controllo”: l’autorità pubblica indipendente istituita da uno Stato membro ai sensi dell’articolo 51;
33. “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;
34. “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;
35. “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.
36. “Istituto o Ente di Ricerca”: un organismo pubblico o privato per il quale la finalità di statistica o di ricerca scientifica risulta dagli scopi dell’istituzione e la cui attività scientifica è documentabile;
37. “ricerca scientifica”: un progetto di ricerca istituito conformemente alle pertinenti norme etiche e metodologiche settoriali, in conformità delle buone prassi.

3. Principi applicabili al trattamento di dati personali

Secondo quanto previsto dall’art. 5 GDPR, i dati personali devono essere:

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*).

L'Ateneo, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento e dei relativi rischi, sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso, mette in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati a tutela dei diritti degli interessati ("*principio di privacy by design*"). Inoltre, per impostazione predefinita i dati personali devono essere trattati nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario ("*principio di privacy by default").*

4. 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, anche per il tramite di attività formative rivolte al personale dell'Ateneo e attività informativa per i soggetti esterni, nel rispetto di quanto previsto dalla normativa, dalle Linee Guida e dai Provvedimenti adottati dal Garante per la Protezione dei Dati Personali.

5. Base giuridica

L'Università è una pubblica amministrazione ai sensi dell'art. 1, c. 2 del D. Lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche.
Pertanto, l'Ateneo tratta i dati personali comuni solo in presenza di una base giuridica che renda lecito tale trattamento e che può consistere:
- nell'esecuzione dei compiti di interesse pubblico e connessi all'esercizio di pubblici poteri attribuiti all'Ateneo da norme di legge o di regolamento;

- nell'adempimento di obblighi contrattuali di cui l'interessato è parte o nell'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- nell'adempimento di obblighi di legge a cui è soggetto l'Università;
- al di fuori dei propri compiti istituzionali, nel perseguimento del legittimo interesse dell'Ateneo o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
- nella salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
- nel consenso dell'interessato, laddove previsto.

Il trattamento di categorie di dati personali da parte dell'Ateneo è vietato, salvo il verificarsi di una delle condizioni indicate dall'art.9, co. 2, del GDPR

6. Dati trattati

Nell'esercizio delle proprie funzioni istituzionali, l'Ateneo tratta con misure adeguate le seguenti tipologie di dati, tenendo conto di quanto disposto da norme di legge e di regolamento:

a) Dati, anche di natura particolare e di carattere giudiziario, 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 (vedasi in allegato Scheda A). 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 sicurezza delle persone nei luoghi di lavoro;
- erogazione del servizio di telefonia fissa e mobile.

b) Dati relativi alla didattica e alla ricerca, compresa la ricerca in ambito medico - sanitario (vedasi in allegato Scheda B).

c) Dati, anche di natura particolare e di carattere giudiziario, relativi a "studenti" intesi nell'accezione più ampia, e per tutte le attività e modalità connesse alla qualità di "studente" e ai laureati (vedasi in allegato Scheda C). 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.

d) Dati relativi alla gestione del contenzioso giudiziale, stragiudiziale e attività di consulenza (vedasi in allegato Scheda D).

e) Dati relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali (con eventuale trattamento di dati particolari e giudiziari). 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

7. Circolazione dei dati all'interno dell'Ateneo

L'Università provvede alla gestione dei dati a sua disposizione mediante strumenti, anche di carattere informatico, che ne facilitino l'accesso e la fruizione. L'accesso e l'utilizzo dei dati all'interno delle strutture e da parte del personale dell'Università, in ragione delle specifiche funzioni assegnate, è ispirato al principio della libera circolazione delle informazioni nell'ottica del raggiungimento delle finalità istituzionali, ferma restando la responsabilità derivante dall'utilizzo improprio degli stessi.

ORGANIZZAZIONE E RESPONSABILITA'

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

8. 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, il 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".

8.1 Compiti e Responsabilità

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

9. Contitolare

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).

10.Responsabile della Protezione dei dati (RPD)

Il RPD è individuato dal Titolare 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.
Per lo svolgimento dei propri compiti il RPD si avvale della collaborazione del personale assegnato al Settore Legale e anche di personale tecnico specializzato afferente all'Area dei Sistemi Informativi.
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 comunicati al Garante per la protezione dei dati personali e sono pubblicati sui siti internet istituzionali nell'apposita sezione denominata "Protezione dei Dati Personali".

10.1 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 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 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:

- disporre tempestivamente di tutta la documentazione e delle 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 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.

11. Responsabile interno (Designato)

L'Ateneo individua 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. 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, nonché tutte le altre figure a queste affini per le quali dovesse rendersi necessaria la formalizzazione di un atto di nomina. 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

12. 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 di supporto all' 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.
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

13. Autorizzato al trattamento

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 sottoscrizione del contratto 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, anche nello svolgimento dell'attività lavorativa a distanza.
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, tenendo presente che sarà l'Ente ospitante a dover formare e autorizzare lo studente al trattamento dei dati nella propria struttura da disciplinarsi nelle singole convenzioni;
- 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 – Settore Legale, 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 ai servizi dell'Università 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.

14. 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.

15. Responsabile Esterno del Trattamento

Il Titolare può avvalersi, per il trattamento di dati, di soggetti pubblici o privati esterni all'Ateneo che, in qualità di Responsabili del trattamento, ai sensi del par. 1 dell'art. 28 del GDPR, eseguono trattamenti per conto del Titolare stesso, fornendo le garanzie previste dalle disposizioni normative, con particolare riferimento all'adeguatezza delle misure tecniche ed organizzative. 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 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. Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dati, il Responsabile conserva nei confronti dell'Università l'intera responsabilità. 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.

SICUREZZA DEL TRATTAMENTO E VIOLAZIONE DATI PERSONALI

16.Misure tecnico-organizzative di sicurezza

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.

a. 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.

17. Violazione dei dati personali ("data breach")

Per violazione dei dati personali, si intende qualsiasi evento, che si traduca in una 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.
Le violazioni che si verificano per trattamenti riguardanti attività svolte dalle Aree dell'Amministrazione Centrale o per trattamenti inerenti alle attività svolte dai Dipartimenti devono essere comunicate senza indugio via e-mail al RPD, all'indirizzo rpd@unimib.it, e comunque entro 24 ore dal fatto. La procedura, nonché la modulistica necessaria a segnalare l'avvenuta violazione, è 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; 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 del Settore Legale, 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 per il trattamento dei dati al fine di verificare il rispetto delle disposizioni del GDPR.

ATTIVITA' E ADEMPIMENTI

18.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 quanti sono le finalità e i trattamenti effettuati.
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.

19.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.

20. 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.

21.Diritti dell'Interessato e modalità di presentazione delle istanze

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 all'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 conservazione 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 il Settore Legale, 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;
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 al Settore Legale nel Sistema di gestione documentale;
    - se l'istanza è pervenuta a mezzo e-mail, sarà cura del Settore Legale richiedere la protocollazione dell'istanza.
3) Viene accertata l'identità dell'istante e la legittimazione dello stesso a presentare l'istanza. Qualora l'istanza venga presentata tramite dominio @campus.unimib.it o @unimib.it, non è richiesta la trasmissione di un documento di riconoscimento in corso di validità del soggetto istante. Viceversa, se l'istanza è presentata tramite un indirizzo mail o PEC non istituzionale, sarà cura dell'Ufficio di Supporto al RPD richiedere l'inoltro del documento di riconoscimento. In caso di esito:
    - negativo, l'istanza viene dichiarata inammissibile con comunicazione all'istante;
    - positivo, l'istanza viene dichiarata ammissibile.
4) Viene comunicata all'interessato la presa in carico dell'istanza ammissibile.
5) Si procede all'istruttoria della pratica, secondo le seguenti fasi

tramite 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, o comunque alla struttura di riferimento;

6) Viene redatto dall'Ufficio di supporto un documento costituente l'istruttoria dell'istanza, sottoscritto dal RPD e sottoposto al vaglio del Titolare;
7) Viene redatto dall'Ufficio di supporto il riscontro formale da inviare all'interessato in base a quanto disposto dal Titolare.
8) 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. Nei periodi di chiusura invernale ed estiva dell'Ateneo, le istanze non potranno essere trattate. 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.

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.

22.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 finali di concorsi (come ad esempio per i concorsi relativi ai docenti e al PTA), nonché negli elenchi con esiti di prove e/o esami di profitto, graduatorie et similia, occorre inserire il nome e il cognome; la data di nascita dovrà essere inserita solo in caso di omonimia e in nessun caso andrà essere 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.

23.Videosorveglianza

l 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.

SANZIONI E RESPONSABILITA'

24.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, come indicato all'art. 83 del GDPR.

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 del D.Lgs. 196/2003, relativamente ai procedimenti giudiziari

25.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.

DISPOSIZIONI ED ENTRATA IN VIGORE

26. 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.

27. 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.

ALLEGATI:

SCHEDA A

Denominazione del trattamento
Gestione del rapporto di lavoro del personale dipendente (docente, dirigente, tecnico–amministrativo), dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato.
Indicazione del trattamento e descrizione riassuntiva del contesto
Sono di seguito descritte le principali caratteristiche: 1. dati inerenti lo stato di salute per esigenze di: gestione del personale, verifica dell'attitudine a determinati lavori, idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, avviamento al lavoro degli inabili, maternità, igiene e sicurezza sul luogo di lavoro, equo indennizzo, causa di servizio, svolgimento di pratiche assicurative e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortunio e/o sinistro, fruizione di particolari esenzioni o permessi lavorativi per il personale dipendente, collegati a particolari condizioni di salute dei dipendenti o dei loro familiari; 2. dati inerenti lo stato di salute dei dipendenti e dei loro familiari acquisiti ai fini dell'assistenza fiscale e dell'erogazione dei benefici socio assistenziali contrattualmente previsti; 3. dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali; 4. dati idonei a rilevare le opinioni politiche o le convinzioni religiose o l'adesione a partiti politici, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale per esigenze connesse alle elezioni ed al riconoscimento di permessi (anche per particolari festività e bandi di concorso), aspettative; 5. dati inerenti l'obiezione di coscienza e le convinzioni inerenti la sperimentazione animale; 6. dati idonei a rivelare l'origine razziale ed etnica ai fini dell'instaurazione e della gestione di rapporti di lavoro con lavoratori stranieri; 7. dati particolari e giudiziari che rilevano nell'ambito di procedimenti disciplinari a carico del personale e, in generale, nei giudizi pendenti di fronte a tutte le giurisdizioni che coinvolgono docenti, dipendenti, collaboratori esterni. E' di seguito descritto sinteticamente il flusso informativo dei dati.

I dati particolari e giudiziari sopra descritti inerenti il rapporto di lavoro, raccolti sia presso gli interessati che presso i terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti dell'Ateneo, sia su base cartacea che su base informatica.

Principali fonti normative

Codice Civile (artt. 2094-2134); **Codice di procedura civile** (artt. 409 e ss.); **R.D. 1038/1933** (*Approvazione del Regolamento di procedura per i giudizi innanzi alla Corte dei Conti);* **L. 96/1955** (*Provvidenze a favore dei perseguitati politici antifascisti o razziali e dei loro familiari superstiti*); **D.P.R. 3/1957** (*Testo unico delle disposizioni concernenti lo statuto degli impiegati civili dello Stato*); **D.P.R. 361/1957** (*Approvazione del testo unico delle leggi recanti norme per la elezione della Camera dei deputati*); **L. 69/1992** (*Interpretazione autentica del comma 2 dell'articolo 119 del testo unico delle leggi recanti norme per la elezione della Camera dei deputati, approvato con D.P.R. 361/1957, in materia di trattamento dei lavoratori investiti di funzioni presso i seggi elettorali*); **D.P.R. 1124/1965** (*Testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali*); **L. 300/1970** (*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento)*; **L. 336/1970** (*Norme a favore dei dipendenti civili dello Stato ed Enti pubblici ex combattenti ed assimilati*); **L. 6 Dicembre 1971 n. 1034** (*Istituzione dei Tribunali amministrativi regionali*); **D.P.R. 1092/1973** (*Approvazione del testo unico delle norme sul trattamento di quiescenza dei dipendenti civili e militari dello Stato*); **L. 200/1974** (*Disposizioni concernenti il personale non medico degli istituti clinici universitari*); **D.P.R. 833/1978** *(Istituzione del servizio sanitario nazionale);* **D.P.R. 761/1979** (*Stato giuridico del personale delle unità sanitarie locali);* **D.P.R. 382/1980** (*Riordinamento della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica*); **L. 14 aprile 1982, n. 164** e successive modifiche (*Norme in materia di rettificazione di attribuzione di sesso*); **L. 8 marzo 1989, n. 101** (*Norme per la regolazione dei rapporti tra lo Stato e l'Unione delle Comunità Ebraiche Italiane*); **L. 205/1990** *(Disposizioni in materia di giustizia amministrativa);* **L. 104/1992** (*Legge quadro per l'assistenza, l'integrazione sociale ed i diritti delle persone handicappate*); **D.Lgs. 502/1992** (*Riordino della disciplina in materia sanitaria, a norma dell'art. 1 della L. 23 Ottobre 1992 n. 421*); **L. 537/1993** (*Interventi correttivi di finanza pubblica*); **D.P.R. 487/1994** *(Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni*); **D.Lgs. 626/1994** (*Igiene e sicurezza sul lavoro*); **L. 335/1995** (*Riforma del sistema pensionistico obbligatorio e complementare*); **D.Lgs. 564/1996** (*Attuazione della delega conferita dall'art. 1, comma 39, della L. 8 Agosto 1995 n. 335, in materia di contribuzione figurativa e di copertura assicurativa per periodi non coperti da contribuzione*); **L. 59/1997** (*Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione*

amministrativa); **D.M. 187/1997** *(Regolamento recante modalità applicative delle disposizioni contenute all'articolo 2, comma 12, della L. 8 Agosto 1995 n. 335, concernenti l'attribuzione della pensione di inabilità ai dipendenti delle amministrazioni pubbliche iscritti a forme di previdenza esclusive dell'assicurazione generale obbligatoria*); **D.P.R. 260/1998** (*Regolamento recante norme per la semplificazione dei procedimenti di esecuzione delle decisioni di condanna e risarcimento di danno erariale, a norma dell'art. 20, comma 8, della L. 15.03.1997 n. 59*); **L. 230/1998** (*Nuove norme in materia di obiezione di coscienza*); **L. 210/1998** *(Norme per il reclutamento dei ricercatori e dei professori universitari di ruolo);* **L. 488/1999** (*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato. Legge Finanziaria 2000*); **L. 68/1999** (*Norme per il diritto al lavoro dei disabili*); **D.Lgs. 517/1999** (*Disciplina dei rapporti fra Servizio sanitario nazionale ed università, a norma dell'articolo 6 della L. 30 novembre 1998 n. 419*); **D.Lgs. 267/2000** *(Testo unico delle leggi sull'ordinamento degli enti locali*); **D.lgs. 445/2000** (*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa)*; **D.Lgs. 165/2001** (*Norme generali sull'ordinamento del lavoro alle dipendenze delle Pubbliche Amministrazioni*); **D.P.R. 461/2001** *(Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonché per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie*); **D.Lgs. 151/2001** *(Testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità, a norma dell'art. 15 della L. 8 Marzo 2000, n. 53*); **D.M. 31 gennaio 2001** (*Procedimento di riscossione dei crediti conseguenti a decisioni di condanna della Corte dei Conti a carico dei responsabili per danno erariale in attuazione dell'art. 4 del D.P.R. 24 giugno 1998 n. 260);* **D.P.R. 334/2004** *(Regolamento recante norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero);* **C.C.N.L.** vigenti del **comparto università**; CCNL del Comparto Sanità; CCNL per ulteriori Comparti specifici, se ed in quanto applicabili; **Statuto di Ateneo**; **Regolamento Generale di Ateneo**; **Regolamento per l'Amministrazione, la Finanza e la Contabilità** ed altri **Regolamenti di Ateneo** vigenti.

Finalità di rilevante interesse pubblico perseguite

Sono contenute nei seguenti articoli del Codice:

- **ART. 112:** "*instaurazione e gestione da parte dei soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato";*

- **ART. 65**: "*applicazione della disciplina in materia di a) elettorato attivo e passivo (...)*";

- **ART 66:** "*applicazione (...) delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti ed ai responsabili d'imposta, nonché in materia di deduzioni e detrazioni*";

- **ART 68:** "*applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni*";

- **ART. 70:** *" applicazione della legge 8 luglio 1998 n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza".*

Caratteristiche del trattamento

- ❑ cartaceo |X|
- ❑ informatico |X|

Tipi di dati PARTICOLARI e/o GIUDIZIARI trattati

- ❑ origine razziale |X| etnica |X|
- ❑ convinzioni religiose, filosofiche, d'altro genere |X|
- ❑ convinzioni politiche, sindacali |X|
- ❑ stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie in corso a fini assicurativi |X|
- ❑ vita sessuale soltanto in relazione ad un'eventuale rettificazione di attribuzione di sesso |X|
- ❑ dati di carattere giudiziario |X|

Operazioni eseguibili

Trattamento "ordinario" dei dati

- ❑ Raccolta: presso gli interessati |X| presso terzi |X|

- ❑ Elaborazione |X| Registrazione |X| Organizzazione |X| Consultazione |X| Modifica |X| Cancellazione |X| Estrazione |X| Blocco |X| Selezione |X| Utilizzo |X|

- ❑ Conservazione |X| Distruzione |X|

Particolari forme di elaborazione

- ❑ Interconnessioni e raffronti di dati: |X|

con altri trattamenti o banche dati appartenenti a Uffici e Strutture dell'Università che si occupano: della gestione del personale, della gestione del contenzioso, della gestione delle risorse finanziarie.

con altri soggetti pubblici o privati:

Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

- ❑ Comunicazione ai seguenti soggetti per le seguenti finalità: |X|

INPDAP – INPS (per erogazione e liquidazione trattamento di pensione, L. 335/1995; L. 152/1968);

Comitato di verifica per le cause di servizio e Commissione medica territorialmente competente (nell'ambito della procedura per il riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001);

INAIL, Autorità di P.S., Sportello unico per l'immigrazione (DPR n. 334/2004) e/o altre Autorità previste dalla legge (per denuncia infortunio, DPR 1124/1965);

Strutture sanitarie competenti (per visite fiscali, art. 21 CCNL del 06/07/1995, CCNL di comparto);

Soggetti pubblici e privati ai quali, ai sensi delle leggi regionali/provinciali, viene affidato il servizio di formazione del personale (le comunicazioni contengono dati particolari soltanto nel caso in cui tali servizi siano rivolti a particolari categorie di lavoratori, ad es. disabili);

Centro per l'impiego o organismo territorialmente competente per le assunzioni ai sensi della legge 68/1999;

Amministrazioni provinciali e Centro regionale per l'impiego in ordine al prospetto informativo delle assunzioni, cessazioni e modifiche al rapporto di lavoro, redatto ai sensi della L. 68/1999;

Autorità giudiziaria (C.P. e C.P.P.);

Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;

Ministero delle Finanze, relativamente alla dichiarazione dei redditi dei dipendenti (art.17 D.M. 164/1999 e art. 2-bis D.P.R. 600/1973);

Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, nell'ambito della mobilità dei lavoratori.

SCHEDA B

Denominazione del trattamento
Attività di ricerca scientifica
Indicazione del trattamento e descrizione riassuntiva del contesto
Sono di seguito descritte le principali caratteristiche: 1. dati particolari e giudiziari trattati nell'ambito delle attività di ricerca inerenti *in toto* le scienze tecniche (agraria, architettura, chimica, biologia, ingegneria), scienze mediche e scienze umanistiche (economiche e sociali, giuridiche, politiche, sociologiche e letterarie), scienze della formazione; 2. dati particolari trattati nell'ambito delle attività didattiche e assistenziali connesse alla ricerca; 3. dati inerenti lo stato di salute acquisiti nell'ambito delle strutture sanitarie convenzionate. E' di seguito descritto sinteticamente il flusso informativo dei dati. I dati particolari e giudiziari inerenti l'attività di ricerca scientifica, contenuti in documenti cartacei, informatici e/o in video-registrazioni, raccolti sia presso gli interessati che presso terzi, possono essere trattati dalle strutture di ricerca e dai ricercatori, di volta in volta designati incaricati o responsabili, sia su base cartacea che su base informatica, mediante le operazioni nel prosieguo meglio descritte. Potranno essere desunti dati particolari anche dal trattamento delle immagini e/o dalle dichiarazioni raccolte nel corso di eventuali video-conferenze, tele-consulti, video-registrazioni o interviste che rappresentano possibili modalità di raccolta dei dati a scopo di ricerca, previa informativa all'interessato sugli scopi dell'iniziativa e sulla volontarietà della partecipazione alla ricerca, avendo cura di specificare nel progetto di ricerca i tipi di dati trattati e le operazioni eseguite in concreto.
Principali fonti normative
L. 398/1989 *(Norme in materia di borse di studio universitarie);* **L. 390/1991** *(Norme sul diritto agli studi universitari*); **L. 449/1997** (*Misure per la stabilizzazione della finanza pubblica*); **D.M. 11.2.1998** (*Determinazione dell'importo e dei criteri per il conferimento di assegni per la collaborazione ad attività di ricerca*); **D.M. 21.5.1998 n. 242**; **D.M. 30.4.1999 n. 224** (*Norme in materia di dottorato di ricerca*); **D.P.C.M. 9.4.2001** (*Disposizioni per l'uniformità di trattamento sul diritto agli studi universitari*); **D.lgs. 517/1999** (*Disciplina dei rapporti fra servizio sanitario nazionale ed università, a norma dell'art. 6 della L. 30 novembre 1998 n. 419*)**; D.P.R. 382/1980** (*Riordino della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica*); **Codice di deontologia e buona condotta per i trattamenti di dati personali per scopi storici del 14.3.2001; Codice di deontologia e buona condotta per i trattamenti di dati personali a scopi statistici e scientifici del 16.6.2004; Accordo finanziario n.**

2004/67/TS; Normativa previdenziale; Normativa fiscale di riferimento; Statuto di Ateneo; **Regolamento Generale di Ateneo**; **Regolamento per l'Amministrazione, la Finanza e la Contabilità** ed altri **Regolamenti di Ateneo** vigenti.

Finalità di rilevante interesse pubblico perseguite

Sono contenute nei seguenti articoli del Codice:

- **ART. 95:** "*istruzione e formazione in ambito scolastico, professionale, superiore o universitario";*

- **ART. 98**: "*trattamenti effettuati da pubblici: per scopi storici (...), per scopi scientifici".*

Caratteristiche del trattamento

- ❑ cartaceo |X|
- ❑ informatico |X|

Tipi di dati PARTICOLARI e/o GIUDIZIARI trattati

- ❑ origine razziale |X| etnica |X|
- ❑ convinzioni religiose, filosofiche, d'altro genere |X|
- ❑ convinzioni politiche, sindacali |X|
- ❑ stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie|X|
- ❑ vita sessuale nell'ambito delle attività di ricerca inerenti le scienze umane e biomediche |X|
- ❑ dati di carattere giudiziario |X|

Operazioni eseguibili

Trattamento "ordinario" dei dati

❑ Raccolta: presso gli interessati |X| presso terzi |X|

❑ Registrazione |X| Organizzazione |X| Conservazione |X| Consultazione |X| Elaborazione* |X| Modificazione |X| Selezione |X| Estrazione |X| Utilizzo |X| Blocco |X| Cancellazione |X| Distruzione |X|

* L'operazione di elaborazione comprende le cautele destinate a rendere anonimo successivamente alla raccolta il dato sensibile e/o giudiziario oggetto di trattamento ai fini della ricerca, a meno che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto nel progetto di ricerca. I risultati della ricerca non possono essere diffusi se non in forma anonima.

Particolari forme di elaborazione

❑ Interconnessioni e raffronti di dati: |X|

con altri trattamenti o banche dati delle Strutture di Ricerca e/o di altri Uffici e Strutture dell'Università.

❑ Comunicazione ai seguenti soggetti: |X|

Altre università, istituzioni e organismi pubblici e privati aventi finalità di ricerca, esclusivamente nell'ambito di progetti congiunti.

Altre università, istituzioni e organismi pubblici e privati, aventi finalità di ricerca e non partecipanti a progetti congiunti, limitatamente ad informazioni prive di dati identificativi e per scopi storici o scientifici chiaramente determinati per iscritto nella richiesta dei dati.

In tali casi, si applicano le ulteriori garanzie previste dagli artt. 8 e 9 del Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e scientifici.

SCHEDA C

Denominazione del trattamento
Attività didattica e gestione delle iscrizioni e delle carriere degli studenti.
Indicazione del trattamento e descrizione riassuntiva del contesto
Sono di seguito descritte le principali caratteristiche: 1. dati relativi agli studenti e/o a familiari diversamente abili o ad elementi reddituali ai fini di un eventuale controllo sulle autocertificazioni relative alle tasse universitarie e di eventuali esoneri dal versamento delle tasse universitarie e/o fruizione di eventuali agevolazioni previste dalla legge, nonché dati relativi alla gestione dei contributi straordinari per iniziative degli studenti; 2. dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio; 3. dati relativi allo stato di gravidanza al fine di attuare tutte le cautele necessarie per la tutela della donna in stato di gravidanza, sia per motivi didattici, quali la frequenza di laboratori, sia al fine della fruizione di eventuali agevolazioni e benefici di legge; 4. dati idonei a rivelare le opinioni politiche o l'adesione a partiti, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale per esigenze connesse allo svolgimento delle procedure elettorali interne all'Ateneo; 5. dati particolari e giudiziari che rilevano nell'ambito di procedimenti disciplinari a carico degli studenti; 6. dati relativi alla condizione di disabile per attività di interpretariato, tutorato, trasporto e servizi analoghi per tutti gli studenti portatori di handicap. E' di seguito descritto sinteticamente il flusso informativo dei dati. I dati particolari e giudiziari sopra descritti inerenti l'attività didattica e la gestione delle iscrizioni e delle carriere degli studenti, raccolti sia presso gli interessati che presso i terzi, vengono trattati dagli Uffici e/o dalle Strutture competenti, sia su base cartacea che su base informatica.
Principali fonti normative

R.D. 1592/1933 e successive modificazioni e integrazioni. (*Testo unico delle leggi sull'istruzione superiore*); **R.D. 1269/1938** e successive modificazioni e integrazioni. *(Approvazione del regolamento sugli studenti);*

D.P.R. 382/1980 (*Riordinamento della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica)*; **L. 168/1989** *(Istituzione del Ministero dell'Università e della Ricerca scientifica e Tecnologica)*; **L. 398/1989** *(Norme in materia di borse di studio universitarie)*; **L. 341/1990** *(Riforma degli ordinamenti didattici universitari)*; **L. 390/1991** *(Norme sul diritto agli studi universitari)*; **L. 104/1992** *(Legge-quadro per l'assistenza, l'integrazione sociale ed i diritti delle persone handicappate)*; **D.M. 224/1999** *(Norme in materia di dottorato di ricerca)*; **D.lgs. 445/2000** (*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa);* **L. 148/2002** *(Ratifica ed esecuzione della Convenzione di Lisbona dell'11 aprile 1997);* **D.M. 270/2004** *(Modifiche al Regolamento recante norme concernenti l'autonomia didattica degli Atenei, approvato con decreto MURST 3 novembre 1999, n. 509)*; **D.P.R. 334/2004** *(Regolamento recante norme di attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulle condizioni dello straniero);* **D.M. 25/3/1998, n. 142** e **L. 24 giugno 1997, n. 196** *(Normativa relativa agli stages);* **DPCM 9 aprile 2001**; **L. 14 febbraio 2003**, **n. 30** (*c.d. Legge Biagi, di riforma del mercato del lavoro*); **Contratto Istituzionale Socrates Erasmus** vigente; **Statuto di Ateneo, Regolamento Generale di Ateneo, Regolamento Didattico di Ateneo, Regolamento per l'Amministrazione, la Finanza e la Contabilità, Regolamento sugli studenti** ed altri **Regolamenti di Ateneo** vigenti; **Leggi Regionali** vigenti in materia di diritto allo studio universitario.

Finalità di rilevante interesse pubblico perseguite

Sono contenute nei seguenti articoli del Codice:

- **ART. 64: "***cittadinanza,immigrazione e condizione dello straniero***"**;
- **ART. 65**: "*applicazione della disciplina in materia di a) elettorato attivo e passivo (...)";*
- **ART. 68: "** *concessione, liquidazione, modifica e revoca di benefici economici, abilitazioni (...)";*
- **ART. 86**: "*...assistenza, integrazione sociale e diritti delle persone handicappate (...)";*
- **ART. 95:** *"istruzione e formazione in ambito scolastico, professionale, superiore o universitario (...)".*

Caratteristiche del trattamento

- ❑ cartaceo |X|
- ❑ informatico |X|

Tipi di dati PARTICOLARI e/o GIUDIZIARI trattati

- ❑ origine razziale |X| etnica |X|
- ❑ convinzioni religiose, filosofiche, d'altro genere |X|
- ❑ convinzioni politiche, sindacali |X|
- ❑ stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie in corso a fini assicurativi |X|
- ❑ vita sessuale soltanto in relazione ad un'eventuale rettificazione di attribuzione di sesso |X|
- ❑ dati di carattere giudiziario |X|

Operazioni eseguibili

Trattamento "ordinario" dei dati

- ❑ Raccolta: presso gli interessati |X| presso terzi |X|
- ❑ Elaborazione |X| Registrazione |X| Organizzazione |X| Consultazione |X| Modifica |X| Cancellazione |X| Estrazione |X| Blocco |X| Selezione |X| Utilizzo |X|
- ❑ Conservazione |X| Distruzione |X|

- ❑ Interconnessioni e raffronti di dati: |X|

  con altri trattamenti o banche dati appartenenti a Uffici e Strutture dell'Università che si occupano della gestione delle risorse finanziarie, della gestione del contenzioso e della gestione dei servizi informatici;

con altri soggetti pubblici o privati: |X|

Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

- ❑ Comunicazione ai seguenti soggetti per le seguenti finalità: |X|

Enti locali ai fini di eventuali sussidi a favore di particolari categorie di studenti, Avvocatura dello Stato, Ministero degli Affari esteri, Questure, Ambasciate, Procura della Repubblica relativamente a permessi di soggiorno, al riconoscimento di particolari status, Regione, altri operatori pubblici e privati accreditati o autorizzati e potenziali datori di lavoro ai fini dell'orientamento e inserimento nel mondo del lavoro (ai sensi della legge 30/2003, sulla riforma del mercato del lavoro, e successive attuazioni), enti di assicurazione per pratiche infortuni.

Organismi Regionali di Gestione (Enti dotati di autonomia amministrativo-gestionale istituiti ai sensi della L. 390/91 in materia di diritto agli studi universitari) ed altri istituti per favorire la mobilità internazionale degli studenti, ai fini della valutazione dei benefici economici e dell'assegnazione degli alloggi (Legge 390/1991 e Leggi regionali in materia).

SCHEDA D

Denominazione del trattamento
Gestione del contenzioso giudiziale, stragiudiziale e attività di consulenza
Indicazione del trattamento e descrizione riassuntiva del contesto
Sono di seguito descritte le principali caratteristiche: 1. dati particolari e giudiziari inerenti i soggetti coinvolti. E' di seguito descritto sinteticamente il flusso informativo dei dati. I dati particolari e giudiziari sopra descritti inerenti la gestione del contenzioso e l'attività di consulenza, raccolti sia presso gli interessati che presso i terzi, vengono acquisiti dagli Uffici preposti e inviati agli Uffici e/o alle Strutture competenti, che operano il trattamento di tali dati sia su base cartacea che su base informatica.
Principali fonti normative
Codice Civile; **Codice di Procedura Civile; Codice Penale; Codice di Procedura Penale; R.D. 642/1907** (*Regolamento per la procedura innanzi alle sezioni giurisdizionali del Consiglio di Stato*); **R.D. 1054/1924** (*Approvazione del testo unico delle leggi sul Consiglio di Stato*); **R.D. 1038/1933** (*Approvazione del Regolamento di procedura per i giudizi innanzi alla Corte dei Conti);* **D.P.R. 3/1957** (*Testo unico delle disposizioni concernenti lo statuto degli impiegati civili dello Stato*); **L. 300/1970** (*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento)*; **L. 336/1970** (*Norme a favore dei dipendenti civili dello Stato ed Enti pubblici ex combattenti ed assimilati*); **L. 1034/1971** (*Istituzione dei Tribunali Amministrativi Regionali*); **L. 689/81** *(Modifiche al sistema penale);* **D.lgs. 285/1992** *(Codice della Strada);* **D.lgs. 546/1992** *(Disposizioni sul Processo Tributario);* **D.P.R. 487/1994** *(Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni*); **L. 335/1995** (*Riforma del sistema pensionistico obbligatorio e complementare*); **D.M. 187/1997** *(Regolamento recante modalità applicative delle disposizioni contenute all'articolo 2, comma 12, della L. 8 Agosto 1995 n. 335, concernenti l'attribuzione della pensione di inabilità ai dipendenti delle amministrazioni pubbliche iscritti a forme di previdenza esclusive dell'assicurazione generale obbligatoria*); **D.P.R. 260/1998** (*Regolamento recante norme per la semplificazione dei procedimenti di esecuzione delle decisioni di condanna e risarcimento di danno erariale, a norma dell'art. 20, comma 8, della L. 15.03.1997 n. 59*);

L. 205/2000 (*Disposizioni in materia di giustizia amministrativa*); **D.lgs. 445/2000** (*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa)*; **L. 241/1990** *(Nuove norme sul procedimento amministrativo);* **D.lgs. 165/2001** (*Norme generali sull'ordinamento del lavoro alle dipendenze delle Pubbliche Amministrazioni*); **D.P.R. 461/2001** *(Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonché per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie*); **D.M. 31 gennaio 2001** (*Procedimento di riscossione dei crediti conseguenti a decisioni di condanna della Corte dei Conti a carico dei responsabili per danno erariale in attuazione dell'art. 4 del D.P.R. 24 giugno 1998 n. 260);* **C.C.N.L.** vigenti del **comparto università; Statuto di Ateneo; Regolamento Generale di Ateneo; Regolamento per l'Amministrazione, la Finanza e la Contabilità** ed altri **Regolamenti di Ateneo** vigenti.

Finalità di rilevante interesse pubblico perseguite

Sono contenute nei seguenti articoli del Codice:

- ART. 71, comma 1, lett. A): " *applicazione delle norme in materia di sanzioni amministrative e ricorsi";*

- ART. 71, comma 1, lett. B): "*far valere il diritto di difesa in sede amministrativa o giudiziaria (...)"*;

- ART. 67, comma 1, lett. A): "*verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia per le quali sono comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti"*.

Caratteristiche del trattamento

- ❑ cartaceo |X|
- ❑ informatico |X|

Tipi di dati PARTICOLARI e/o GIUDIZIARI trattati

- ❑ origine razziale |X| etnica |X|
- ❑ convinzioni religiose, filosofiche, d'altro genere |X|
- ❑ convinzioni politiche, sindacali |X|
- ❑ stato di salute: patologie attuali, patologie pregresse, dati sulla salute relativi anche ai familiari, terapie in corso |X|
- ❑ vita sessuale |X|
- ❑ dati di carattere giudiziario |X|

Operazioni eseguibili

Trattamento "ordinario" dei dati

- ❑ Raccolta: presso gli interessati |X| presso terzi |X|
- ❑ Elaborazione |X| Registrazione |X| Organizzazione |X| Consultazione |X| Modifica |X| Cancellazione |X| Estrazione |X| Blocco |X| Selezione |X| Utilizzo |X|
- ❑ Conservazione |X| Distruzione |X|

Particolari forme di elaborazione

- ❑ Interconnessioni e raffronti di dati: |X|

  con altri trattamenti o banche dati appartenenti a Uffici e Strutture dell'Università

  che si occupano: della gestione del personale, della gestione delle risorse finanziarie, della gestione dell'attività didattica e di ricerca, della stipula-esecuzione dei contratti e della gestione delle procedure formali ed informali di scelta del contraente.

- ❑ Comunicazione ai seguenti soggetti per le seguenti finalità: |X|

Avvocatura Distrettuale e Generale dello Stato, ai fini della gestione del contenzioso penale, civile ed amministrativo;

Autorità Giudiziaria di qualsiasi ordine e grado, arbitri, Amministrazioni interessate ai fini della gestione dei ricorsi straordinari al Presidente della Repubblica, Organi di Polizia giudiziaria, Commissioni Tributarie, Uffici Provinciali del Lavoro ai fini del tentativo obbligatorio di conciliazione;

Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte quando dovuto;

Compagnie di assicurazione, in caso di polizze assicurative che prevedano tali comunicazioni.