UNIVERSITÀ DEGLI STUDI DI TORINO

DIREZIONE AFFARI GENERALI

Decreto Rettorale n. 870 del 04/03/2019

OGGETTO: **"Regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio".**

IL RETTORE

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" e successive modifiche ed integrazioni;

Richiamato lo Statuto dell'Università degli Studi di Torino, emanato con D.R. n. 1730 del 25 marzo 2012;

Visto il Decreto Legislativo del 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", come novellato dal D. Lgs. 10 agosto 2018, n. 101;

Richiamato il Regolamento di Attuazione del Codice in materia di Protezione dei Dati, emanato con Decreto Rettorale del 24 febbraio 2006, n. 143, con cui si dava attuazione al Codice in materia di Protezione dei Dati disposto con il Decreto Legislativo n. 196 del 30 giugno 2003;

Richiamato il Regolamento di Ateneo per il trattamento dei dati sensibili e giudiziari ai sensi del Decreto Legislativo 196/2003, emanato con decreto Rettorale del 12 marzo 2007, n. 1819;

Visto il Regolamento Europeo (UE) 27 aprile 2016, n. 679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 ed entrato in vigore il 25 maggio 2018, 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 Decreto Legislativo del 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)";

Vista la deliberazione del Consiglio di Amministrazione n. 2/2019/III/1 del 26 febbraio 2018 con la quale è stato approvato il testo del "*Regolamento* in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio";

Valutato ogni opportuno elemento;

DECRETA

di emanare il "*Regolamento* in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio", quale parte integrante del presente Decreto, e che lo stesso regolamento entra in vigore il quindicesimo giorno successivo alla data di pubblicazione sull'albo on line di Ateneo.

Visto: la Direttrice della Direzione Affari Generali

Il RETTORE
Prof. Gianmaria AJANI

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO UE 27 APRILE 2016, N. 679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO E DEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.

ARTICOLO 1
AMBITO DI APPLICAZIONE

1. Il presente Regolamento, adottato in attuazione del Regolamento UE n. 2016/679 (di seguito "Regolamento UE") e del D. Lgs. n. 196/2003 come novellato dal D. Lgs. n. 101/2018 (di seguito "Codice in materia di protezione dei dati personali"), disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi di cui è titolare l'Università degli Studi di Torino (di seguito "Università").
2. L'Università in qualità di titolare del trattamento effettua i trattamenti di dati con o senza ausilio di processi automatizzati.
3. I dati sono trattati nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.
4. I trattamenti effettuati dall'Università per il raggiungimento dei propri fini istituzionali non necessitano del consenso dell'interessato e trovano fondamento nella condizione di liceità prevista dall'art. 6, paragrafo 1, lett. b), e) del Regolamento (UE).
5. L'Università effettua il trattamento dei dati personali in modo lecito, corretto e trasparente, come azione prioritaria al fine di instaurare e mantenere un rapporto di fiducia con gli studenti, il personale e i terzi interessati.
6. Tutti coloro che trattano dati personali all'interno dell'Università perché espressamente autorizzati o per l'espletamento di compiti propri della struttura cui funzionalmente afferiscono, dovranno effettuare il trattamento nel rispetto del principio di riservatezza e di protezione dei dati personali in attuazione del presente Regolamento.

ARTICOLO 2
DEFINIZIONI

Si intende per:
1. **trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
2. **comunicazione:** dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies* del Codice in materia di dati personali, al trattamento dei dati personali sotto l'autorità' diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
3. **diffusione:** dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

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, o l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale;
6. **dati genetici**: i dati personali relative alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
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. **dato anonimo:** la normativa europea e nazionale in materia di protezione dei dati personali non si applica alle informazioni "anonime", ossia quelle informazioni raccolte senza alcun riferimento ad una persona fisica identificata o identificabile a cui il dato potrebbe riferirsi;
10. **anonimizzazione:** misura di sicurezza tecnica volta a impedire irreversibilmente l'identificazione dell'interessato a cui i dati si riferiscono. A seconda della tecnica utilizzata e dalle misure di sicurezza definite all'interno di apposite *policies*, i dati anonimizzati potrebbero rientrare nell'ambito di applicazione della normativa di protezione dati personali.
11. **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;
12. **responsabile esterno**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
13. **responsabile interno**: i responsabili delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono. All'interno dell'Ateneo i responsabili interni sono così individuati:
    - per le strutture amministrative: la Direttrice Generale, per i dati relativi alle proprie attività, e le/i Direttrici/Direttori delle Direzioni per le attività di propria competenza;
    - per le Strutture di didattica e di ricerca: le/i Direttrici/Direttori dei Dipartimenti e le/i Direttrici/Direttori delle Scuole delle scuole e le/i Direttrici/Direttori dei Centri di 1° livello;
14. **referente privacy:** figura di supporto al responsabile interno per agevolare l'attuazione degli adempimenti in materia di protezione dei dati delle persone fisiche, facenti capo al responsabile interno al trattamento dei dati;

15. **responsabile della transizione al digitale**: figura i cui compiti sono definiti dall'art. 17, comma 1-sexies del Codice dell'Amministrazione Digitale (emanato con D.lgs. n.82 del 7 marzo 2005, quale risultante dalle successive modifiche e integrazioni, inclusa l'ultima disposizione integrativa e correttiva di cui al decreto legislativo 13 dicembre 2017, n. 217);
16. **responsabile della conservazione dei documenti informatici**: figura 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, inclusa l'ultima disposizione integrativa e correttiva di cui al decreto legislativo 13 dicembre 2017, n. 217);
17. **amministratore di sistema (AdS):** figura professionale individuata nell'ambito informatico, finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti ma anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
18. **responsabile prevenzione della corruzione e della trasparenza**: figura individuata dall'organo di indirizzo politico tra dirigenti amministrativi di ruolo di prima fascia in servizio, ai sensi dell'art. 1, co. 7 L. n. 190/2012.
19. **autorizzati al trattamento**: le persone fisiche formalmente autorizzate e istruite a trattare i dati personali sotto l'autorità diretta e per le finalità stabilite dal Titolare e/o del Responsabile interno e/o Responsabile esterno (artt. 4, 29, 32, 39 del Regolamento UE);
20. **interessato al trattamento**: la persona fisica, la persona giuridica, l'ente o l'associazione 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 inequivocabile, 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 esterno del trattamento, il responsabile interno del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
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. **pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali 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 tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
26. **cifratura:** misura tecnica di sicurezza informatica applicabile ai dati personali da parte del Titolare, destinata a rendere tali dati incomprensibili a chiunque non sia autorizzato ad accedervi.

27. **limitazione di trattamento:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro (art. 4 paragrafo 3 e Considerando 67 del Regolamento UE);
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. **responsabile per la protezione dei dati**: figura specializzata nel supporto al Titolare del trattamento prevista come obbligatoria negli enti pubblici;
30. **registro attività di trattamento**: elenco, in forma cartacea o digitale, delle attività di trattamento dei dati personali effettuate sotto la propria responsabilità dal Titolare e dal Responsabile esterno per la protezione secondo le rispettive competenze;
31. **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;
32. **violazione dei dati personali**: la violazione di 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;
33. **stabilimento principale**: come definito dall'art. 4, paragrafo 16 e dai Considerando 36 e 37 del Regolamento UE. Per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
34. **rappresentante**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta per quanto riguarda gli obblighi rispettivi ai sensi del Regolamento UE sulla protezione dei dati personali;
35. **impresa**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
36. **gruppo imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
37. **norme vincolanti d'impresa**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
38. **autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51. L'autorità italiana preposta è il Garante per la protezione dei dati personali;
39. **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, ovvero il 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;

40. **autorità di controllo interessata**: un'autorità di controllo interessata al trattamento di dati personali 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; c) oppure un reclamo è stato proposto a tale autorità di controllo;
41. **obiezione pertinente e motivata**; un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
42. **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;
43. **messa a disposizione:** forma di trattamento con riferimento a documenti, regolamenti di attuazione e *policies*: consiste nel rendere conoscibili procedure, documenti e informazioni a categorie definite di destinatari interessati, al fine di consentirne l'applicazione (es. pubblicazione per condivisione tramite intranet di Ateneo);
44. **privacy by design:** principio introdotto dall'art. 25 del Regolamento UE per cui il Titolare, al momento di determinare i mezzi del trattamento di dati personali, mette in atto misure tecniche ed organizzative adeguate volte ad attuare in maniera efficace i principi di protezione dati, per assicurare il rispetto del Regolamento UE e la tutela delle persone fisiche;
45. **privacy by default:** principio introdotto dall'art. 25 del Regolamento UE per cui il Titolare del trattamento di dati personali, all'atto del trattamento stesso, mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione e la minimizzazione, e integra nel trattamento le necessarie garanzie a tutela degli interessati.

ARTICOLO 3
PRINCIPI

1. Il trattamento dei dati personali viene effettuato dall'Università in applicazione dei principi previsti dall'art. 5 del Regolamento (UE).
2. In particolare, i dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità ("limitazione della finalità"). Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
d) esatti e, se necessario, aggiornati. A tal fine sono adottate 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, e a condizione dell'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE ("limitazione della conservazione");

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale, compresa la protezione, mediante misure tecniche e organizzative adeguate ("integrità e riservatezza");
3. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, l'Università adotta misure tecniche e organizzative adeguate in grado di comprovare il rispetto dei principi di cui al precedente comma ("principio di responsabilizzazione del Titolare").

ARTICOLO 4
BASE GIURIDICA DEL TRATTAMENTO

1.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 il trattamento di dati personali nell'esercizio dei suoi compiti istituzionali trova il fondamento di liceità nella condizione prevista dall'art. 6, paragrafo 1 lett. e) del Regolamento (UE). Il trattamento è lecito se è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
2. La base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è costituita esclusivamente da una norma di Legge o, nei casi previsti dalla Legge, di Regolamento, secondo quanto previsto dall'art. 2-*ter*, c. 1 del Codice in materia di protezione dei dati personali.
3. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato ("principio di necessità").

ARTICOLO 5
CIRCOLAZIONE DEI DATI ALL'INTERNO DELL'UNIVERSITÀ

1. L'accesso e l'utilizzo dei dati all'interno delle strutture e da parte del personale dell'Università è ispirato al principio della libera circolazione delle informazioni in funzione del raggiungimento delle finalità istituzionali.
2. L'Università provvede alla gestione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione.
3. L'accesso ai dati personali all'interno delle strutture e da parte del personale dell'Università, connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, è consentito in via diretta e tracciato senza ulteriori formalità nella misura necessaria e al solo fine del perseguimento dell'interesse istituzionale, ferma restando la responsabilità del richiedente derivante dall'utilizzo improprio dei dati e nell'ottica del bilanciamento tra i diritti e le libertà dell'interessato e l'interesse pubblico all'espletamento delle attività istituzionali.

ARTICOLO 6
TIPOLOGIE DI DATI TRATTATI DALL'UNIVERSITÀ

1.L'Università effettua, con misure adeguate e tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto, delle finalità del trattamento, trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali, come individuate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Regolamento (UE), dal Codice in materia di protezione dei dati personali e dalle Linee guida e dai provvedimenti dell'Autorità nazionale garante per la protezione dei dati personali.
2. L'Università tratta a titolo esemplificativo e non esaustivo:
A. dati personali comuni;

B. dati personali, anche di natura particolare, con riferimento a determinati servizi 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 e relativo 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 di welfare e per la fruizione di agevolazioni,
- salute e la sicurezza delle persone nei luoghi di lavoro,
- erogazione del servizio di telefonia fissa e mobile,
- procedimenti di natura disciplinare a carico del personale;

C. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi a studenti intesi nell'accezione più ampia, per tutte le attività e modalità connesse allo status di studente:

- 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 al conseguimento del titolo),
- 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,
- servizi di mobilità studenti in ingresso ed in uscita;

D. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi alla didattica e alla ricerca (compresa la ricerca scientifica in ambito medico - sanitario);

E. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali:

- 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,
- accesso a servizi federati.

3. É compito dei Responsabili interni con il supporto e la collaborazione dei Referenti privacy aggiornare e documentare il censimento periodico dei trattamenti in atto e segnalare eventuali nuovi trattamenti.

ARTICOLO 7
TITOLARE DEL TRATTAMENTO DEI DATI

1. Il Titolare del trattamento dei dati è l'Università nel suo complesso nella persona del rappresentante legale protempore: il Magnifico Rettore.
2. L'Università adotta misure tecniche e organizzative adeguate al fine di garantire ed essere in grado di dimostrare la conformità del trattamento al Regolamento (UE) e al Codice in materia di protezione dei dati personali, tenendo conto della natura, dell'ambito di applicazione, del contesto, della base giuridica e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le misure tecniche ed organizzative sono definite in apposite linee guida o *policies* oggetto di periodico aggiornamento, tenuto conto dello stato dell'arte e dell'evoluzione tecnologica.
Tali *policies* riguarderanno anche il trattamento dei dati nelle sedute degli Organi Collegiali.
Le misure tecniche sono predisposte e aggiornate dalla Direzione Sistemi Informativi, Portale, E-learning e quelle organizzative dalle Strutture competenti per materia.
3. Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, l'Università assicura che non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento (UE) trasferendo i dati personali a Paesi terzi o organizzazioni internazionali definiti adeguati dalla Commissione europea sulla base di una decisione ai sensi dell'art. 45 del Regolamento (UE), ovvero, in mancanza, potrebbe trasferire i dati personali fornendo garanzie adeguate che permettano il riconoscimento di diritti azionabili e mezzi di ricorso effettivi. (artt. 46 e 49 del Regolamento UE).
4. L'Università è tenuta a cooperare con il Garante per la protezione dei dati personali, così come disposto agli artt. 157-160 del Codice di protezione dati personali.

ARTICOLO 8
CONTITOLARE

1. Quando uno o più titolari del trattamento determinano congiuntamente con l'Università le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.
2. L'Università e il Contitolare del trattamento stabiliscono in modo trasparente, mediante un accordo interno, le rispettive responsabilità e i rispettivi obblighi derivanti dal Regolamento (UE), con particolare riguardo all'esercizio dei diritti dell'interessato, nonché le rispettive funzioni di comunicazione delle informazioni richieste dall'Informativa privacy, salvo quanto previsto dall'art. 26 del Regolamento (UE).
3. L'accordo definisce adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione da ciascun Contitolare nei confronti degli interessati anche mediante forme di pubblicazione.
4. L'interessato può esercitare i propri diritti nei confronti di ciascun contitolare del trattamento.

ARTICOLO 9
IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD) O DATA PROTECTION OFFICER (DPO)

1. L'Università in qualità di ente pubblico ha l'obbligo di nominare ai sensi dell'art. 37 del Regolamento (UE) un Responsabile della protezione dei dati (di seguito "RPD").
2. Il RPD è figura specializzata nel supporto al Titolare in materia di trattamento dati personali e svolge la funzione di raccordo con il Garante per la protezione dei dati personali e di garante per i soggetti interessati.
3. Il RPD è individuato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti.

4. Il RPD può essere un soggetto interno (dipendente dell'Università) o esterno, assolvendo in tal caso i suoi compiti in base a un contratto di servizi.
5. Il RPD è nominato, nel caso di soggetti interni, con decreto del Rettore.
6. Il RPD è tenuto a svolgere i seguenti compiti:
a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa comunitaria e nazionale relativa alla protezione dei dati;
b) sorvegliare sulle politiche del Titolare del trattamento, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) sorvegliare sull'osservanza delle disposizioni derivanti dal regolamento UE, dalla normativa comunitaria e nazionale relativa alla protezione dei dati personali e dai Regolamenti di Ateneo in materia;
d) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati personali e sorvegliarne l'effettivo svolgimento e completamento;
e) segnalare al Titolare ed al Direttore Generale:
- le priorità di intervento in relazione alle novità normative e tecniche
- eventuali inadempienze emerse in occasione dell'espletamento delle funzioni istituzionali;
f) cooperare con il Garante per la protezione dei dati personali;
g) fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento (UE), ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
h) cooperare in ottica di *"accountability"* con il Titolare per la definizione delle istruzioni da impartire ai fini dell'adempimento degli obblighi in materia di trattamento dei dati personali e per le attività di informazione e formazione, rivolte alle strutture competenti, in merito alla tenuta del Registro delle attività di trattamento (c.d. Registro dei Trattamenti);
7. Il RPD e lo Staff posto a Suo supporto non possono avere compiti gestionali od organizzativi. L'adeguamento al Regolamento UE è posto a carico di tutte le Direzioni e delle Strutture competenti per ambito, sulla base delle istruzioni impartite dal Titolare nei rispettivi atti di nomina a Responsabile interno e con il supporto dei Referenti Privacy.
8. Nell'eseguire i propri compiti il RPD considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
9. L'Università deve mettere a disposizione del RPD risorse necessarie e adeguate a garantire lo svolgimento ottimale dei propri compiti, avvalendosi delle competenze e della collaborazione delle strutture universitarie. È costituita a tal fine un'Unità di Staff a supporto del RPD che ne è responsabile per l'espletamento delle attività di consulenza e di vigilanza nell'interesse del Titolare. Lo Staff per il supporto al RPD è sottoposto gerarchicamente al Titolare del trattamento, nella persona del Magnifico Rettore tenendo conto del vigente Regolamento Generale di Organizzazione di Ateneo non può essere investito di compiti gestionali, né si occupa dell'adeguamento normativo dei trattamenti di dati personali.
10. Il RPD ha libero accesso ai dati e deve essere informato in relazione alle problematiche inerenti la protezione dei dati personali ed alle attività che impattano sul trattamento dei dati, fin dalla fase di progettazione. I Direttori della Direzione Sistemi Informativi, Portale, E-learning e della Direzione Ricerca e Terza Missione supportano il RPD nelle sue attività per progetti ed attività che comportino trattamenti di dati personali strettamente legati all'evoluzione tecnologica ed all'attività di ricerca.

11. L’Università garantisce che il RPD eserciti le proprie funzioni in modo autonomo e indipendente e in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o in conflitto di interesse con la sua posizione.
12. Il RPD non riceve alcuna istruzione per quanto riguarda l’esecuzione dei compiti a lui affidati ai sensi dell’art. 39 del Regolamento (UE).
13. L’Università non rimuove o penalizza il RPD in ragione dell’adempimento dei compiti affidati nell’esercizio delle sue funzioni.
14. Il nominativo e i dati di contatto del RPD sono comunicati al Garante per la protezione dei dati personali. I dati di contatto del RPD sono indicati nelle informative privacy e pubblicati sul sito internet istituzionale.
15. L’Università costituisce a supporto del RPD una rete di Referenti Privacy che dovranno collaborare funzionalmente con il RPD, nell’ambito delle strutture di appartenenza presso cui sono nominati a cura del Responsabile interno al trattamento.
16. Su indicazione del RPD possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali.
17. Il RPD redige periodicamente una relazione in merito all’attività svolta, tenuto conto di questioni che impattano con priorità ed urgenza sul trattamento dei dati e riferisce almeno una volta all’anno al Consiglio di Amministrazione ed al Rettore.

ARTICOLO 10
RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI

1.È Responsabile esterno del trattamento qualunque soggetto esterno che esegua, in base a un contratto/convenzione o altro atto giuridico, trattamenti di dati personali per conto dell’Università e risponde in solido con l’Università in caso di inadempienze.
2. In forza di delega di firma attribuita dal Titolare ai responsabili interni del trattamento (“delega dal lato attivo”), il contratto o atto giuridico che documenta la nomina a Responsabili esterni del trattamento, è sottoscritto dai Responsabili interni in relazione alle competenze di funzione, connesse al contratto/convenzione originale, da cui deriva l’obbligo di designazione.
3. Nei casi in cui l'Università degli Studi di Torino, sulla base di impegni contrattuali, effettua trattamenti di dati per conto di terzi, il responsabile interno del trattamento corrispondente è nominato dai partners responsabile esterno al trattamento dati (“delega dal lato attivo”).
4. La nomina, conforme al diritto nazionale, fornisce le garanzie ai sensi dell'art. 28, paragrafo 3 del Regolamento (UE), con particolare attenzione alle misure tecniche e organizzative adeguate a soddisfare le istruzioni fornite dal Titolare, in funzione della liceità del trattamento e a tutela dei diritti e delle libertà dell’interessato. Al responsabile esterno è richiesto di fornire informazioni documentate volte a garantire adeguati livelli di conformità rispetto alla normativa vigente in materia.
5. Il Responsabile esterno, in applicazione dell‘art. 28 del Regolamento (UE) può ricorrere ad un altro Responsabile del trattamento (di seguito “sub-responsabile”) per l’esecuzione di specifiche attività di trattamento da svolgersi per conto del Titolare.
Il Responsabile esterno può ricorrere ad un eventuale sub-responsabile previa autorizzazione scritta, specifica o generale, del Responsabile interno in conformità al contratto o atto giuridico, che contiene la nomina a Responsabile esterno e tenuto conto delle garanzie fornite dal sub-responsabile in termini di trattamento e protezione dei dati.
6. Qualora un sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile esterno iniziale conserva nei confronti dell’Università l'intera responsabilità dell'adempimento degli obblighi che ne derivano.
7. Il Responsabile esterno risponde dinanzi all’Università dell’inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni derivanti dall’attività di trattamento.

ARTICOLO 11
RESPONSABILI INTERNI DEL TRATTAMENTO DEI DATI PERSONALI

1. Sono individuati quali Responsabili interni del trattamento dei dati personali, sulla base delle competenze attribuite alla rispettiva funzione organizzativa o carica istituzionale che ricoprono, i Responsabili delle Strutture nell'ambito delle quali i dati personali sono trattati per le finalità istituzionali.
2. I Responsabili interni sono così individuati:
   - per le strutture amministrative: la Direttrice Generale, per i dati relativi alle proprie attività, e le/i Direttrici/Direttori delle Direzioni per le attività di propria competenza;
   - per le strutture di didattica e di ricerca: le/i Direttrici/Direttori dei Dipartimenti e le/i Direttrici/Direttori delle Scuole delle scuole e le/i Direttrici/Direttori dei Centri di 1° livello;

3. Il Responsabile interno, opportunamente formato riguardo alle competenze anche decisionali in materia di trattamento dei dati, opera con autonomia gestionale nell'ambito delle competenze affidategli, collabora funzionalmente con il RPD per l'espletamento dei seguenti compiti all'interno della propria struttura di afferenza e per gli ambiti espressamente definiti:

- con riferimento al personale assegnato:
  - individuare e nominare per iscritto i soggetti autorizzati al trattamento dei dati personali, identificati nelle persone che operano nella Struttura assegnata, secondo le rispettive competenze;
  - individuare e designare in base alla complessità della struttura ed all'eterogeneità dei dati trattati, da due a dieci persone di riferimento (Referenti Privacy) che avranno il compito di supporto e raccordo nei rapporti fra il Direttore ed il Responsabile per la protezione dei dati personali di Ateneo RPD per gli adempimenti previsti dalla normativa vigente;
  - aggiornare periodicamente l'elenco degli stessi e rendere disponibile la documentazione relativa alla nomina nella pagina Intranet di Ateneo nella sezione Privacy dedicata;
  - fornire agli autorizzati specifiche istruzioni operative riguardanti le operazioni di raccolta, trattamento e archiviazione dei dati personali su supporto informatico e cartaceo e individuare puntualmente l'ambito di trattamento consentito;
  - vigilare e verificare che gli autorizzati rispettino le istruzioni impartite e garantire che il trattamento dei dati avvenga in modo lecito e corretto, nel rispetto dei principi di cui all'art. 5 del Regolamento (UE);
  - vigilare sul rispetto delle misure di sicurezza da parte del personale autorizzato, al fine di evitare rischi, anche accidentali, di distruzione o perdita di dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del trattamento;
  - garantire la formazione del personale autorizzato e l'aggiornamento periodico autorizzando gli stessi a partecipare a corsi ed eventi formativi organizzati dall'Università di Torino in materia di protezione dei dati;
- con riferimento ai dati trattati:
  - attenersi scrupolosamente alle disposizioni previste dal Regolamento UE e alle procedure, istruzioni, fac-simili predisposte in materia di privacy dal Titolare del trattamento e consultabili all'interno della sezione intranet dedicata;
  - redigere ed aggiornare l'elenco delle tipologie dei dati trattati nell'ambito della Struttura di competenza e trasmetterlo al Titolare e al RPD;

- comunicare al Titolare e al RPD con adeguato preavviso, anche nel caso di passaggio dalla modalità cartacea a quella elettronica, eventuali nuovi trattamenti, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, anche nel caso di passaggio dalla modalità cartacea a quella elettronica;
- comunicare al Titolare e al RPD le modifiche relative alle attività di trattamento dei dati, nonché gli eventuali mutamenti organizzativi o tecnici (acquisizione di nuove banche dati e/o applicativi hardware, etc.) che possano avere impatto rispetto ai diritti dell'interessato;
- collaborare per la mappatura dei trattamenti, per il censimento delle banche dati e dei trattamenti dei dati esternalizzati, limitatamente a quelli riferibili alla Struttura di propria competenza, ai fini dell'aggiornamento del Registro dei trattamenti;
- garantire, per ciascun trattamento riferibile alla Struttura di propria competenza, che siano sempre rispettati i principi generali previsti dalla normativa vigente in materia e in particolare che i dati siano esatti, aggiornati e completi;
- assicurare che i dati da pubblicare sul sito istituzionale, siano conformi alla normativa vigente in materia e siano rispettati gli obblighi di trasparenza e tracciabilità, come previsto dal Codice di comportamento dell'Università degli Studi di Torino (D.R. n. 646/2016);
- valutare, insieme agli Amministratori di sistema e in coerenza con le policy stabilite dal Responsabile della Conservazione di Ateneo, i tempi di conservazione dei dati, ovvero, se non è possibile, i criteri utilizzati per determinare tale periodo;

● con riferimento alle misure di sicurezza:

- incaricare i Referenti Privacy per individuare e censire i trattamenti soggetti a maggiori rischi di impatto rispetto alle libertà ed ai diritti degli interessati e validare gli aggiornamenti delle schede destinate ad alimentare il registro dei trattamenti;
- informare, senza ingiustificato ritardo, secondo la policy di Ateneo in materia di sicurezza informatica, il Responsabile della Sicurezza Informatica di Ateneo e per conoscenza il Titolare, dopo aver avuto notizia di qualsiasi violazione che potrebbe compromettere il corretto trattamento e la sicurezza dei dati (anomalie, furti, perdite accidentali o distruzioni dei dati) al fine di attivare, nel caso sia riscontrato un rischio grave per i diritti e le libertà delle persone fisiche, la procedura del Data Breach;
- gestire e documentare tramite un apposito registro interno le violazioni dei dati personali riferibili alla propria Struttura di competenza, comprese le circostanze ad esse relative, le loro conseguenze e tutti i provvedimenti adottati per porvi rimedio;
- rispettare e far rispettare le misure di sicurezza tecniche indicate e adottate dalla Direzione Sistemi Informativi, Portale, E-learning e le misure di sicurezza organizzative previste dalle normative vigente e dai provvedimenti del Garante, nonché eventuali misure ritenute adeguate su proposta del Titolare, atte a preservare la disponibilità e integrità del dato;
- verificare periodicamente in collaborazione con la Direzione Edilizia, Logistica e Sostenibilità, le modalità di accesso ai locali e le misure adottate per la protezione delle aree logistiche in termini di custodia ed accessibilità ai dati (ad esempio: supporti di videosorveglianza), al fine di garantire la sicurezza e la riservatezza degli archivi cartacei;

● con riferimento ai diritti degli interessati:

- vigilare sull'aggiornamento e/o redazione dell'informativa di cui artt. 13 e 14 del Regolamento (UE), da fornire agli interessati, secondo quanto disciplinato di seguito all'art. 15 del presente Regolamento;

- integrare l’informativa e i moduli di consenso, nel caso di trattamenti specifici, sentito il Titolare e il Responsabile della protezione dati;
- gestire e riscontrare, nei termini previsti dalla normativa vigente, le istanze per l’esercizio dei diritti dell’interessato (diritto accesso, rettifica, cancellazione, limitazione al trattamento etc..), in collaborazione con tutti gli uffici coinvolti nel trattamento del dato oggetto della richiesta;

4. Il Responsabile interno deve altresì provvedere all’espletamento di tutte le operazioni necessarie per il rispetto e la corretta applicazione della normativa europea e nazionale vigente in materia, collaborare nelle fasi connesse alla valutazione di impatto sui trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone, ai sensi dell’art. 35 del Regolamento (UE);
5. Il Responsabile interno è tenuto a partecipare direttamente alle iniziative formative organizzate dall’Amministrazione sul tema della protezione dei dati.
6. Il Responsabile interno nell’ambito dei suoi poteri gestionali e di controllo, deve collaborare attivamente con i il Titolare e con il Responsabile della protezione dati in caso di eventuali ispezioni da parte dell’Autorità Garante e delle altre Autorità di controllo.
7. La nomina a Responsabile interno è strettamente correlata all’incarico conferito, non è delegabile e decade in caso di dimissioni dal ruolo ricoperto ovvero per revoca da parte del Titolare del trattamento, la quale dovrà essere motivata e potrà essere disposta in ipotesi di gravi violazioni, anche senza preavviso. Tale nomina non prevede alcuna remunerazione aggiuntiva.
8. Della nomina sarà data evidenza mediante pubblicazione dell’elenco dei nominativi dei Responsabili interni nella pagina intranet di Ateneo alla sezione dedicata.

ARTICOLO 12
REFERENTI PRIVACY

1. I Referenti privacy in materia di trattamento dei dati, sono nominati previa individuazione da parte dei singoli Responsabili interni delle Strutture organizzative, con decreto Rettorale.
2. I Referenti privacy svolgono i compiti attribuiti in materia di trattamento dei dati senza vincoli di responsabilità, nel pieno esercizio delle ordinarie attività amministrativo/gestionali già assegnate.
3. I Referenti privacy svolgono il ruolo di facilitatori per esaminare e segnalare le criticità che emergono all’interno delle singole Strutture di riferimento negli ambiti concernenti il trattamento e la protezione di dati. Assumono all’interno delle singole Strutture di riferimento una posizione di raccordo nei rapporti con i colleghi e i collaboratori rispetto alle attività prescritte in materia di trattamento dati e nei rapporti tra il Direttore ed il Responsabile per la protezione dei dati personali.
4. I Referenti privacy in materia di trattamento dei dati sono tenuti a svolgere i seguenti compiti:
- collaborare nel censimento dei trattamenti dei dati di competenza della Struttura di afferenza e vigilare sulla corretta compilazione delle schede destinate ad alimentare il registro dei trattamenti;
- collaborare all'aggiornamento del registro dei trattamenti dati;
- individuare in collaborazione con gli uffici competenti della Struttura di afferenza, i rapporti contrattuali con i fornitori esterni, in linea con la normativa europea ed italiana relativa al trattamento dei dati (art. 28 Regolamento UE);
- in collaborazione con gli uffici competenti della Struttura, verificare l’esistenza delle nomine a Responsabili esterni del trattamento nei casi di esternalizzazioni dei servizi (art. 28 Regolamento UE, aggiornare e/o revisionare la documentazione presente, ovvero collaborare nella redazione delle stesse se mancanti;

- in collaborazione con gli uffici competenti della Struttura, verificare l'esistenza delle informative al trattamento dei dati ai sensi degli artt. 13 e 14 del Regolamento (UE), aggiornare e/o revisionare la documentazione presente, ovvero collaborare nella redazione delle stesse se mancanti;
- comunicare preventivamente, ossia prima dell'avvio, al Responsabile interno e al Responsabile di riferimento della Direzione Sistemi Informativi, Portale, E-learning (nei casi di trattamenti informatizzati) e alla Direzione Edilizia, Logistica e Sostenibilità (nei casi dei trattamenti cartacei), l'attivazione di un nuovo trattamento, dandone notizia al Responsabile della protezione dati (RPD) nei casi di trattamenti più complessi;
- supportare nella revisione e/o predisposizione di adeguate policy e sorvegliare sulla corretta applicazione delle stesse;
- informare in modo tempestivo, qualora si verifichi qualsiasi evento che possa compromettere la sicurezza dei dati trattati: (anomalie, furti, distruzione, divulgazione/accessi non autorizzati, perdite accidentali di dati) al fine di attivare la procedura del Data Breach che prevede la notifica all'Autorità Garante entro 72 ore nei casi in cui la violazione comporti gravi rischi per i diritti e le libertà delle persone fisiche (artt. 33 e 34 del Regolamento UE);
- supportare la Direzione competente nel censimento degli impianti di videosorveglianza installati nelle aree logistiche della Struttura di afferenza;
- supportare il Responsabile interno nella gestione del registro delle violazioni dei dati personali riferibili alla Struttura di appartenenza, di cui sia venuto a conoscenza su segnalazione del soggetto autorizzato al trattamento.

5. I Referenti privacy sono tenuti a seguire corsi di formazione ed aggiornamento. Ai fini della opportuna rendicontazione, sono tenuti a partecipare alle riunioni e/o incontri organizzati dallo Staff RPD per i temi da trattare in materia di protezione dei dati e sicurezza dei dati.
6. La nomina di Referente Privacy non comporta alcuna modifica della qualifica professionale o delle mansioni e non determina remunerazione aggiuntiva.
7. La nomina di Referente privacy ha la durata di un anno e può essere rinnovata sulla base della rendicontazione degli obblighi di formazione, di informazione e delle attività svolte in adempimento dei compiti prescritti.
8. L'elenco dei Referenti Privacy è pubblicato nella pagina intranet alla Sezione dedicata e viene aggiornato periodicamente.

ARTICOLO 13
AUTORIZZATI AL TRATTAMENTO

1. Il Responsabile interno al trattamento dati, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, designa espressamente il personale docente, il personale tecnico amministrativo e il personale non strutturato, come soggetti autorizzati e impartisce loro specifiche istruzioni.
2. 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 in occasione della sua attività lavorativa;
- a non comunicare a terzi, a non diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza in veste di autorizzato;
- a seguire i seminari di informazione e formazione in materia di protezione dei dati personali e a sostenere i relativi test finali per la verifica dell'apprendimento;
- a segnalare con tempestività al proprio Responsabile di ufficio e al Referente Privacy 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, la procedura del Data Breach;
- a seguire le linee guida/*policies* adottate dall'Ateneo e a consultare periodicamente la sezione intranet dedicata;
- In caso di ispezioni da parte dell'Autorità Garante, della Polizia Postale e della Guardia di Finanza, qualora si verifichi un intervento immediato o si abbia conoscenza della notizia di ispezione, avvisare tempestivamente il proprio responsabile gerarchico e il Referente Privacy della Struttura di afferenza, al fine di informare ed attivare la filiera dei soggetti responsabili e offrire la massima collaborazione nelle attività ispettive, fornendo la documentazione richiesta e ogni altra informazione utile di cui si abbia legittimamente cognizione.

Ulteriori istruzioni sono dettagliate nell'atto di nomina dei soggetti autorizzati, a cura del Responsabile interno della Struttura di afferenza, sotto la propria responsabilità e in relazione a specifici compiti e funzioni connessi al trattamento dati.

3. L'autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio, può nei casi previsti dalla legge integrare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari, oltre che esporre l'Amministrazione a danni anche reputazionali, oltre che patrimoniali.

4. L'autorizzato si impegna a osservare la normativa europea e nazionale vigente in materia, i Regolamenti, le istruzioni e le policies adottate dall'Università, ogni altro atto in tema di trattamento dati e le relative istruzioni impartite per i trattamenti di dati con e senza strumenti elettronici, definite nel presente articolo e negli atti di nomina.

ARTICOLO 14
SENSIBILIZZAZIONE E FORMAZIONE

1. Ai fini della corretta e puntuale applicazione della disciplina in materia di protezione dei dati personali, l'Università sostiene e promuove, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore dei dati personali. L'Università promuove l'attività formativa di tutto il personale universitario e fornisce idonee informazioni a tutti coloro che hanno rapporti con l'Amministrazione o l'Ente nel suo complesso.

2. L'Università predispone ogni anno, sentito il Responsabile per la protezione dati, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata. Tale formazione è integrata e coordinata con le attività pianificate in materia di prevenzione della corruzione nonché in tema di trasparenza e di accesso agli atti, ai documenti, ai dati ed alle informazioni.

3. Ogni sessione formativa prevede, nell'ottica della responsabilizzazione, una prova finale di apprendimento.

4. La frequenza alle attività di formazione è obbligatoria.

ARTICOLO 15
INFORMATIVA

1. Per ogni tipologia di trattamento dei dati l'Università fornisce l'informativa all'interessato, ai sensi degli artt. 13 e 14 del Regolamento (UE). L'informativa fornita all'interessato deve essere concisa, trasparente, intelligibile, facilmente accessibile e deve essere usato un linguaggio chiaro e semplice.

2. Nell’ipotesi in cui i dati siano raccolti presso l’interessato, l’informativa deve essere data nel momento in cui i dati personali sono ottenuti, e deve contenere:
- l’identità e i dati di contatto dell’Università;
- i dati di contatto del Responsabile della Protezione dei Dati personali;
- le finalità del trattamento;
- la base giuridica del trattamento ai sensi dell’art. 6 del Regolamento (UE);
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l’indicazione dell’eventuale trasferimento dei dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di una decisione di adeguatezza alla base del trasferimento, ovvero il riferimento alle garanzie adeguate, i mezzi per ottenere una copia di tali dati ed il luogo dove sono stati resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti che l’interessato può esercitare, quali: l’accesso ai dati personali, la rettifica, la cancellazione, la limitazione del trattamento, l’opposizione al trattamento, la portabilità dei dati, il diritto di proporre reclamo al Garante per la protezione dei dati personali e in generale tutti i diritti previsti dagli artt. da 15 a 22 del Regolamento (UE);
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale, la natura obbligatoria o facoltativa del conferimento con l’indicazione delle possibili conseguenze in caso di mancato conferimento di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.
3. Nel caso in cui i dati personali già raccolti devono essere trattati ulteriormente per una finalità diversa da quella per cui sono stati ottenuti, l’Università, prima di attivare l’ulteriore trattamento, fornisce all'interessato informazioni in merito alla diversa finalità. Tale disposizione non si applica se e nella misura in cui l’interessato già dispone dell’informazione, ovvero quando: comunicare una nuova informazione in merito alla diversa finalità, risulta impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fermo restando che l’ulteriore finalità del trattamento non sia incompatibile con le finalità iniziali in conformità all’art. 5 lett. b) e all’art. 89 del Regolamento (UE).
In tali casi l’Università adotta misure appropriate per tutelare, i diritti, le libertà e i legittimi interessi dell’interessato, anche rendendo pubbliche le informazioni.
4. L’attivazione di ogni nuovo trattamento dati comporta l’obbligo di rilasciare una nuova informativa in relazione alle finalità perseguite.
5. Nel caso in cui i dati non siano raccolti presso l’interessato, l’informativa deve contenere oltre che gli elementi suindicati anche le categorie di dati trattati e le relative fonti di provenienza. In questa ipotesi l’informativa deve essere fornita:

- entro un termine ragionevole dall’ottenimento dei dati personali, e comunque non oltre un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- non oltre la prima comunicazione all’interessato, se i dati personali sono destinati alla comunicazione stessa;
- non oltre la prima comunicazione dei dati personali, se è prevista la comunicazione ad altro destinatario.

6. L’aggiornamento o la redazione delle informative di competenza delle Strutture rientra nei compiti di vigilanza del Responsabile interno con il supporto dei Referenti privacy.
7. Il personale e chiunque operi sotto l’autorità dell’Università può trattare i dati personali solo per le specifiche finalità indicate nell’informativa fornita all’interessato al momento del conferimento dei dati o per ogni altra finalità prevista dalla legge.

ARTICOLO 16
DIRITTI DELL'INTERESSATO

1. L'Università garantisce il rispetto dei diritti degli interessati di cui agli artt. da 15 a 22 del Regolamento (UE). In particolare l'interessato può nei confronti del Titolare del trattamento:
a) ottenere la conferma dell'esistenza o meno di trattamenti di dati personali che lo riguardano, e la loro comunicazione in forma intelligibile ("diritto di accesso");
b) ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa ("diritto di rettifica");
c) ottenere la cancellazione dei dati personali che lo riguardano, raccolti in forma cartacea o digitale, senza ingiustificato ritardo nonché esercitare il diritto all'oblio in ipotesi di indicizzazione dei dati, chiedendo la cancellazione degli stessi qualora sussista almeno una delle seguenti condizioni indicate dall'art. 17 del Regolamento (UE):

- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono trattati illecitamente;
- i dati sono trattati per l'adempimento ad un obbligo legale;
- i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione e riguardano minori.

L'Università informa della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione ("diritto alla cancellazione e diritto all'oblio");
d) esercitare il diritto alla limitazione del trattamento come previsto dall'art.18 del Regolamento (UE) ("diritto di limitazione");
e) ottenere la portabilità dei dati forniti nei casi in cui è prevista l'applicazione ai sensi dell'art. 20 del Regolamento (UE) ("diritto alla portabilità");
f) esercitare il diritto di opposizione ("diritto di opposizione");
g) esercitare il diritto di non essere sottoposto ad una decisione basato su un trattamento automatizzato, compresa la profilazione, secondo quanto previsto dall'art. 22 del Regolamento (UE) ("diritto a non essere sottoposto ad un processo decisionale automatizzato");
h) proporre reclamo all'autorità di controllo, secondo quanto previsto dall'art. 77 del Regolamento (UE) ("diritto di reclamo").
2. L'interessato può esercitare i suoi diritti con richiesta indirizzata al Responsabile della struttura competente alla gestione dei dati personali oggetto della richiesta o, in alternativa, al Responsabile interno della Struttura stessa o suo Referente, secondo i dati di contatto indicato nelle informative di riferimento.
3. Il riscontro alla richiesta presentata dall'interessato viene fornito dal destinatario della richiesta, come indicato nel comma precedente, in riferimento alla Struttura che ha la gestione del dato di cui si tratta, senza ingiustificato ritardo e comunque entro 30 giorni dalla data di acquisizione della richiesta al Protocollo, anche nei casi di diniego.
Per i casi di particolare e comprovata difficoltà il termine dei 30 giorni può essere prorogato per altri 2 mesi, non ulteriormente prorogabili. Di tale proroga deve essere data informazione motivata all'interessato entro un mese dall'acquisizione della richiesta al Protocollo.
4. Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.
5. L'Università agevola, per il tramite dei Responsabili interni o loro Referenti, l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa.
6. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.

7. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, l'Università può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi sostenuti oppure può rifiutare di soddisfare la richiesta, dimostrando il carattere manifestamente infondato o eccessivo della stessa. Il Consiglio di amministrazione stabilisce i criteri per la definizione delle modalità di pagamento e dell'importo del contributo spese da parte degli interessati.
8. I Responsabili interni con la collaborazione dei Referenti privacy devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi, nei casi più complessi, del supporto del Responsabile della protezione dati. La modulistica per la presentazione delle istanze è disponibile sul sito nazionale dell'autorità Garante e viene richiamata nelle pagine web del portale dell'Università.
9. Le richieste di esercizio di diritti da parte degli interessati devono essere inserite entro e non oltre 30 giorni dalla data di conclusione del procedimento all'interno di un Registro la cui gestione è affidata ad ogni struttura per le richieste di rispettiva competenza.
10. Nei casi di trattamenti di dati esternalizzati, il Responsabile esterno è tenuto a collaborare con l'Università in sede di riscontro delle istanze di esercizio dei diritti presentate dall'interessato e segnalare le stesse con tempestività.

ARTICOLO 17
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

1. È vietato trattare ai sensi dell'art. 9 del Regolamento (UE) dati personali atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, fatti salvi i seguenti casi:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali, per una o più finalità specifiche;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato alla finalità perseguita;
g) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali conformemente alla normativa nazionale in materia o ad un contratto con un professionista della sanità;
h) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria nel rispetto dei diritti e delle libertà dell'interessato;
i) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità con l'art. 89, paragrafo 1, 2 del Regolamento (UE).

Le misure di garanzia sui dati genetici, biometrici e relativi alla salute, sono definite con apposito provvedimento dal Garante per la protezione dei dati personali, secondo quanto previsto dal Codice in materia di protezione dei dati personali.
Per una disciplina di dettaglio in proposito si rinvia ad apposito Regolamento di Ateneo.

ARTICOLO 18
TRATTAMENTO DI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

1. Il trattamento di dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza, deve avvenire solo sotto il controllo dell'autorità pubblica, se è autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento.
2. Per una disciplina di dettaglio in proposito si rinvia ad apposito Regolamento di Ateneo.

ARTICOLO 19
ACCESSO AI DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO

1. L'accesso del pubblico ai documenti ufficiali è un trattamento considerato di interesse pubblico e i dati personali, contenuti in documenti conservati presso l'Università, possono essere comunicati nei casi previsti dalla legge al fine di conciliare in riferimento al singolo caso concreto l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi dell'art. 86 del Regolamento (UE).
2. Per i presupposti, le modalità e i limiti relativi all'esercizio del diritto di accesso si richiamano le disposizioni vigenti in materia di Trasparenza amministrativa.

ARTICOLO 20
COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI

1. L'Università può comunicare ad altre pubbliche amministrazioni e diffondere, anche sui propri siti web: i nominativi del proprio personale e dei collaboratori, informazioni sul ruolo ricoperto, i recapiti telefonici e gli indirizzi telematici istituzionali.
2. Fermo restando le norme vigenti in materia di accesso ai documenti amministrativi, e le norme vigenti in materia di scambio di dati tra enti pubblici, la comunicazione di dati è sempre ammessa per i fini istituzionali ove prevista da norma di legge o, nei casi previsti dalla legge, di regolamento, ai sensi dell'art. 2-*ter* del Codice in materia di protezione dei dati personali, ovvero, in mancanza, quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali.
3. L'Università, al fine di agevolare l'orientamento, le esperienze formative e professionali e l'eventuale collocazione nel mondo del lavoro, anche all'estero, può, su richiesta degli interessati, comunicare o diffondere, anche a privati e per via telematica: dati relativi agli esiti formativi, intermedi e finali degli studenti e altri dati personali diversi da quelli previsti dagli artt. 9 e 10 del Regolamento UE, dati ed elenchi riguardanti studenti, diplomati, laureandi e laureati, specializzati, borsisti, dottorandi, assegnisti, e altri profili formativi, nonché di soggetti che hanno superato l'esame di stato.
4. L'Università può comunicare altresì, a finanziatori di borse di dottorato e assegni, anche stranieri, dati comuni relativi a dottorandi e assegnisti che abbiano usufruito dei finanziamenti.
5. In considerazione del sistema di autovalutazione, accreditamento e valutazione periodica dei Corsi di studio definito dal MIUR, l'Università può elaborare e/o comunicare le opinioni degli studenti sulla didattica agli organismi deputati ad effettuare verifiche della qualità della didattica quali il Nucleo di Valutazione o il Presidio della Qualità. Tali dati sono trattati con lo scopo di definire azioni volte al miglioramento della qualità della didattica.

ARTICOLO 21

TRATTAMENTI NELL'AMBITO DEL RAPPORTO DI LAVORO

1. L'Università effettua il trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi.
2. L'Università garantisce ai dipendenti l'esercizio dei diritti previsti dagli articoli da 12 a 22 del Regolamento (UE).
3. L'Università adotta misure tecniche e organizzative atte a garantire la tutela delle prerogative individuali e sindacali come disposte dalla normativa italiana, in particolare dallo Statuto dei lavoratori e dalle norme che lo richiamano, oltre che dalle regole deontologiche promosse dal Garante per la protezione dei dati personali.
4. L'Università può comunicare a soggetti pubblici e privati dati comuni del personale che, in ragione di una qualità professionale specifica, usufruisce di corsi di formazione forniti in accordo con altri Enti pubblici, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.
5. Nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile, successivo all'invio del curriculum stesso.
6. Non è dovuto il consenso da parte dell'interessato al trattamento dei dati personali presenti nei curricula spontaneamente trasmessi, quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

ARTICOLO 22
COMUNICAZIONE E DIFFUSIONE DEI DATI RELATIVI AD ATTIVITÀ DI STUDIO E DI RICERCA

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico l'Università può, ai sensi dell'art.100 del Codice in materia di protezione dei dati personali, comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei trattamenti di categorie particolari di dati personali e dei trattamenti dei dati personali relativi a condanne penali e reati .
2. I dati relativi ad attività di studio e di ricerca, non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241 e possono essere trattati per i soli scopi in base ai quali sono comunicati o diffusi.
3. L'Università può comunicare eventuali informazioni inerenti la produttività scientifica, i riconoscimenti e i fondi acquisiti da singoli, da gruppi o da specifici settori scientifico-disciplinari, anche nell'ambito di procedure di valutazione di richieste di finanziamento o di progetti di ricerca, al fine di:
a) promuovere modelli di programmazione delle attività di ricerca e di allocazione delle risorse secondo meccanismi che consentano di garantire trasparenza nella definizione delle priorità, di valorizzare adeguatamente le capacità dei singoli e dei gruppi e di rispettare i principi di trasparenza ed equità di trattamento;
b) favorire la cooperazione tra singoli e gruppi mediante una precisa conoscenza dei risultati conseguiti, allo scopo di migliorare la capacità di attrarre finanziamenti esterni o di istituire forme di collaborazione strutturata con soggetti terzi;
c) fornire orientamento e sostegno per lo sviluppo di modelli organizzativi di supporto alla ricerca, anche tramite la realizzazione di analisi comparative e la condivisione di buone pratiche.
4. L'Università può comunicare dati personali a soggetti pubblici che abbiano erogato dei finanziamenti per la ricerca, ai fini di rendicontazione e per consentire elaborazioni statistiche.

ARTICOLO 23
DIFFUSIONE DELLE VALUTAZIONI D'ESAME

1. In ottemperanza ai principi di trasparenza cui l'Università si ispira e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, è consentita la pubblicazione dei dati inerenti alle valutazioni d'esame anche sui siti web di Ateneo.
2. La pubblicazione dei dati di cui al comma precedente sui siti web è consentita unicamente mediante la diffusione del numero di matricola dello studente e del voto conseguito, nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.
3. I tempi di pubblicazione sono definiti da apposite linee guida o *policies* nel rispetto della normativa vigente.

ARTICOLO 24
DIFFUSIONE DEI RISULTATI DI CONCORSI E SELEZIONI

1. In ottemperanza ai principi di trasparenza cui l'Università si ispira, è consentita la pubblicazione di esiti di prove concorsuali e selettive, nonché delle relative graduatorie, anche sui siti web di Ateneo.
2. La pubblicazione dei dati sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati.
3. Nel caso di diffusione delle valutazioni sui siti web di Ateneo, tali informazioni sono pubblicate per un periodo di tempo non superiore a sei mesi.

ARTICOLO 25
TRATTAMENTO AI FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE, DI RICERCA SCIENTIFICA O STORICA O A AI FINI STATISTICI

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto dei diritti e delle libertà dell'interessato in applicazione del principio della minimizzazione dei dati, delle relative autorizzazioni generali del Garante e dei relativi codici deontologici in materia.
2. I dati dovranno essere trattati con misure tecniche e organizzative adeguate che non consentano di identificare l'interessato, al solo scopo di perseguire le finalità di archiviazione nel pubblico interesse o di ricerca storica.
3. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42, dalle relative regole deontologiche, dai Regolamenti di Ateneo in materia e da apposite linee guida o *policies*.
4. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali di dati sono stati in precedenza raccolti o trattati, secondo quanto previsto dall'art. 99 del Codice in materia di protezione dei dati personali.
Per il raggiungimento di tali finalità, possono essere conservati o ceduti ad altro titolare, i dati personali dei quali, per qualsiasi causa, è cessato il trattamento, nel rispetto di quanto previsto dall'art. 89 paragrafo 1 del Regolamento (UE).

ARTICOLO 26
TRATTAMENTO AI FINI DI RICERCA MEDICA, BIOMEDICA ED EPIDEMIOLOGICA

1. Non è necessario il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea, ivi incluso il caso in cui la ricerca rientri in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-*bis* del d.lgs. 30 dicembre 1992, n. 502, e sia condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento (UE).
2. Il consenso non è altresì necessario quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure vi sia un rischio reale di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il Responsabile scientifico della ricerca adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Il progetto di ricerca deve essere sottoposto a preventiva consultazione del Garante per la protezione dei dati personali.
3. In caso di esercizio del diritto di rettifica e integrazione dei dati personali da parte dell'interessato, la rettifica e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produca effetti significativi sul risultato della ricerca.
4. Ai fini del trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici, si applica quanto disposto dall'art. 110-*bis* del Codice in materia di protezione dei dati personali.

ARTICOLO 27
SICUREZZA

1. L'Università mette in atto misure tecniche ed organizzative adeguate per garantire livelli di sicurezza contro l'eventuale rischio di violazione dei diritti e delle libertà delle persone fisiche connesso al trattamento dei dati personali.
2. Nel valutare l'adeguato livello di sicurezza, l'Università tiene conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, oltre che della probabilità e gravità del rischio derivante dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'Università, effettua la valutazione dei rischi connessi al trattamento e adotta misure di sicurezza comprendenti, tra le altre:
- la pseudonimizzazione e la cifratura dei dati,
- le misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni;
- la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino per garantire la disponibilità e l'accesso in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4. Un gruppo di lavoro costituito con Decreto Rettorale e coordinato dal Direttore dei Sistemi Informativi, ha il compito di definire, sulla base della valutazione dei rischi, le metodologie in ordine all'applicazione delle misure tecniche e organizzative e relazionare sullo stato della sicurezza privacy in Ateneo.
5. Le misure tecniche sono definite tramite apposite linee guida o *policies*, riesaminate e aggiornate periodicamente, tenuto conto dello stato dell'arte e dell'evoluzione tecnologica, sono pubblicate sulla rete intranet nella sezione dedicata e illustrate nelle sessioni formative.
6. L'Università considera rischioso l'esportazione e l'archiviazione di dati personali su ogni supporto (computer portatili, copie cartacee, pendrive, etc.). Il rischio risulta più elevato per le categorie particolari di dati, per grandi volumi di dati personali e per le informazioni che comportano particolari rischi per l'interessato nel caso di perdita o distruzione.

7. I dati possono essere esportati fuori dagli ambienti dell'Università esclusivamente in circostanze eccezionali documentate e motivate e sotto la diretta responsabilità del Responsabile della Struttura,
8. Per quanto non espressamente disciplinato dal presente articolo in materia di sicurezza dei dati, si rinvia a quanto disposto dai regolamenti di Ateneo, dalle policies privacy di Ateneo adottate anche sulla base delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte da AgID e successive modifiche.

ARTICOLO 28
REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

1. Il titolare del trattamento dati, in applicazione dell'art. 30 paragrafo 1 del Regolamento (UE), ha l'obbligo di tenere ed aggiornare, un Registro delle attività di trattamento svolte sotto la propria responsabilità. È onere di ogni Direzione e Struttura alimentare e aggiornare il sopra citato Registro con i dati di propria competenza.
2. Il Registro censisce le attività di trattamento svolte all'interno di ciascuna Strutture dell'Università e costituisce strumento preliminare rispetto all'analisi del rischio.
Il registro è costantemente aggiornato, pubblicato sulla rete intranet di Ateneo nella sezione dedicata e, su richiesta è messo a disposizione dell'Autorità Garante per la protezione dei dati personali, in caso di controlli ed ispezioni.
3. Il Registro dei trattamenti dei quali l'Università è Titolare contiene le seguenti informazioni:

- il nome ed i dati di contatto del Titolare del trattamento, del contitolare ove esistente, del RPD, dei Responsabili interni e dei loro Referenti privacy;
- le finalità del trattamento;
- la descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od un'organizzazione internazionale;
- l'eventuale trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, la descrizione delle misure di sicurezza tecniche ed organizzative del trattamento adottate, ai sensi dell'art. 27 del presente Regolamento e dell'art. 32 del Regolamento (UE).

4. Nei casi in cui l'Università in qualità di responsabile esterno, agisce per conto di terzi nelle attività connesse al trattamento dati, ha l'obbligo in applicazione dell'art. 30 paragrafo 2, di tenere ed aggiornare, uno specifico Registro delle corrispondenti attività di trattamento.
Il Registro contiene le seguenti informazioni:

- il nome ed i dati di contatto dell'Università in qualità di responsabile esterno, di ogni titolare del trattamento per conto del quale agisce l'Università, del RPD;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 del Regolamento (UE), la documentazione delle garanzie adeguate;
- la descrizione generale delle misure di sicurezza tecniche ed organizzative del trattamento adottate sulla base del contratto o atto giuridico che definisce la nomina a Responsabile esterno.

ARTICOLO 29
LA VALUTAZIONE DI IMPATTO PRIVACY

1. Quando un tipo di trattamento prevede l’uso di nuove tecnologie e considerati la natura, l'oggetto, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Responsabile interno, previa consultazione con il RPD, effettua, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali.
2. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.
3. La valutazione d'impatto sulla protezione dei dati è obbligatoria 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 suddette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali quali: l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona, dati relativi a condanne penali e a reati;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza);
d) il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico;
e) in tutti gli altri casi previsti dalla Linee Guida del Comitato dei Garanti europei che indicano anche ipotesi in cui la valutazione di impatto è facoltativa, ma consigliata.
4. Il Responsabile interno con il supporto del Referente privacy, può consultare il RPD e richiedere un parere in merito alla decisione di effettuare o meno la valutazione di impatto. Il parere del RPD costituisce documento da allegare all’atto della valutazione di impatto, fermo restando l’obbligo del responsabile interno di motivare la sua decisione qualora si discosti dal parere espresso dal RPD.
5. Il Responsabile per la Sicurezza e per la transizione al digitale fornisce supporto ai Responsabili interni o loro Referenti e collabora con il RPD ai fini dello svolgimento della valutazione di impatto privacy, anche con compiti di vigilanza.
6. Se necessario il Responsabile interno procede ad un riesame per valutare se il trattamento dei dati, sia effettuato conformemente alla valutazione di impatto sulla protezione dei dati, almeno quando insorgono variazioni del rischio, rappresentato dalle attività relative al trattamento.
7. L’Università, per il tramite del RPD, consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della valutazione di impatto (DPIA) condotta indicano l’esistenza di un rischio residuale elevato.
8. L’Università, per il tramite del RPD, consulta il Garante per la Protezione dei dati personali anche nei casi espressamente previsti dalla normativa vigente in materia.

ARTICOLO 30
VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

1. La violazione dei dati personali si configura nei casi in cui si verifica una violazione di sicurezza che comporti 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.

2. Al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati, l'Università in qualità di Titolare del trattamento definisce una procedura di gestione delle violazioni di dati personali, definita Data Breach.
3. Tale procedura si applica a qualunque attività svolta dall'Università con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.
4. La procedura definisce le modalità per identificare la violazione, analizzare le cause della violazione, definire le misure da adottare per rimediare alla violazione dei dati personali, attenuarne i possibili effetti negativi, registrare le informazioni relative alla violazione, identificare le azioni correttive e valutarne l'efficacia.
In caso di accertata e documentata violazione dei dati personali, l'Università è tenuta a notificare all'Autorità Garante senza ingiustificato ritardo e ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza. L'obbligo della notifica non sussiste in capo all'Università quando risulta improbabile che la violazione dei dati personali presenti un rischio per i diritti e la libertà delle persone fisiche (art. 33 del Regolamento UE).
Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e la libertà delle persone fisiche, l'Università è tenuta a comunicare la violazione all'interessato senza ingiustificato ritardo.
5. La procedura è ratificata dal Consiglio di Amministrazione ed è resa disponibile attraverso la rete intranet di Ateneo nella sezione dedicata.
L'Università pianifica sezioni di informazioni e formazione finalizzate ad illustrare la procedura del Data Breach, in termini di ruoli, compiti, responsabilità e sanzioni.
6. Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste in attuazione della stessa può comportare nei casi più gravi, provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

ARTICOLO 31
VIDEOSORVEGLIANZA

1. L'Università può utilizzare, in qualità di ente pubblico, gli impianti di videosorveglianza per finalità istituzionali, di didattica e di ricerca. L'Università può utilizzare tali impianti ai sensi e nel rispetto di quanto stabilito all'art. 4, c. 1 e 2, della L. 300/1970 e ss.mm. (cd. "Statuto dei lavoratori").
Gli impianti di videosorveglianza possono essere utilizzati altresì per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'ente
2. Il trattamento effettuato tramite i sistemi di videosorveglianza dovrà, in ogni caso, rispettare i principi elencati all'art. 5 del Regolamento (UE), così come quanto stabilito nel provvedimento del Garante sulla videosorveglianza del 10 aprile 2010 ed eventuali successive modifiche, nonché le norme indicate nella regolamentazione di Ateneo di riferimento.
3. Il trattamento di dati personali connesso agli impianti di videosorveglianza deve essere effettuato altresì nel rispetto:

- del principio di proporzionalità, nella scelta delle modalità di ripresa e dislocazione, nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite;
- del principio di necessità, il quale comporta un obbligo di attenta configurazione di **sistemi informativi e di programmi informatici** per ridurre al minimo l'utilizzazione di dati personali.

4. Le strutture, nel rispetto del principio di *accountability*, sono tenute a individuare, documentare e verificare la necessità, le finalità e le caratteristiche dell'installazione delle telecamere.

5. Le strutture comunicano, con congruo preavviso, la creazione, la modifica o la dismissione degli impianti di videosorveglianza alla Direzione Edilizia, Logistica e Sostenibilità, che ha il compito di censimento, gestione e manutenzione dei suddetti impianti, di monitoraggio compreso quello di audit della relativa cartellonistica e informativa. La Direzione Edilizia, Logistica e Sostenibilità, in sinergia con la Direzione Sistemi Informativi, Portale, E-Learning, verificano l'adeguatezza delle misure di sicurezza tecniche dell'impianto e il relativo aggiornamento. Le sopra citate Direzioni adottano e aggiornano le relative policies in materia.
6. I dati personali raccolti tramite il sistema di videosorveglianza potranno essere comunicati in caso di indagini alla polizia giudiziaria o altra autorità competente.
7. I soggetti autorizzati al trattamento di dati personali connessi ai sistemi di videosorveglianza, sono tenuti a partecipare alle iniziative di informazione e ai corsi di formazione in materia, in armonia con quanto previsto dalla normativa vigente in tema di protezione dei dati personali.
8. Solo il personale autorizzato può avere accesso alle immagini ed è sottoposto a tutti i vincoli di riservatezza previsti dall'atto di nomina che ha ricevuto nonché ad applicare scrupolosamente e diligentemente le istruzioni fornite.
9. La conservazione delle immagini deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi, in ogni caso non superiori alla settimana nel rispetto delle indicazioni del Garante. Solo in alcuni casi, per peculiari esigenze tecniche o per la particolare rischiosità dell'attività svolta dal titolare del trattamento, nonché su richieste delle competenti autorità, può ritenersi ammesso un tempo più ampio di conservazione dei dati.
10. Resta ferma la necessità di effettuare una valutazione di impatto (DPIA), nei casi previsti dalla normativa e dalle Linee guida dei Garanti europei e nazionale, ai sensi dell'art. 30, comma 3, lettera c) del Regolamento (UE), ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.

ARTICOLO 32
SANZIONI AMMINISTRATIVE

1. Fermo restando quanto previsto dagli artt. 58, 82, 83 e 84 del Regolamento (UE) e dall'art. 166 del Codice in materia di protezione dei dati personali, le sanzioni disciplinari e amministrative a carico del personale in caso di violazione delle leggi e delle procedure in tema di protezione dei dati personali saranno definite dall'Università anche sulla base di quanto disposto dai CCNL, dal Codice etico e dai Codici di comportamento.

ARTICOLO 33
TRATTAMENTO DEI DATI NELLE SEDUTE DEGLI ORGANI COLLEGIALI DI ATENEO

1. Nelle sedute degli Organi Collegiali dell'Università il trattamento dei dati avviene in conformità al presente Regolamento e al solo fine delle attività istruttorie per le finalità deliberative di competenza.
2. Per la trattazione di argomenti inerenti lo sviluppo strategico dell'Ateneo, i rapporti con gli operatori economici e altri soggetti privati e la tutela della riservatezza dei dati personali, è esclusa, in applicazione del regolamento europeo sulla protezione dei dati personali, la diffusione in qualsiasi forma, ivi compreso lo streaming e le videoriprese, ferma restando l'informazione sulle decisioni degli Organi.
3. Il Presidente dell'Organo Collegiale può avvalersi della consulenza del Responsabile della Protezione dei Dati.

ARTICOLO 34
DISPOSIZIONI FINALI

1. Il presente Regolamento è approvato dal Consiglio di Amministrazione ed emanato con Decreto Rettorale e sostituisce il previgente “Regolamento di Attuazione del Codice in materia di protezione dei dati personali” D.R. n. 143 del 24/02/2006.
2. Dalla data di entrata in vigore del presente Regolamento, devono intendersi abrogate tutte le norme regolamentari incompatibili in relazione a soggetti e materie interessate al trattamento, comprese quelle di regolamenti di funzionamento degli Organi Collegiali.
3. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento UE e del Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di indirizzo, dalle privacy policies di Ateneo e dalle Regole deontologiche adottate e approvate dal Garante per la protezione dei dati personali.
4. Costituiscono parte integrante e sostanziale del presente Regolamento tutti gli allegati che ad esso si riferiscono in quanto connessi ad ambiti specifici in esso contenuti, anche redatti successivamente alla sua emanazione.

ARTICOLO 35
EFFICACIA TEMPORALE E PUBBLICITÀ

1. Il presente Regolamento entra in vigore il quindicesimo giorno successivo alla data di pubblicazione sull'albo on line di Ateneo.
2. L'Università provvede a dare pubblicità al presente Regolamento ed alle successive modifiche ed integrazioni mediante pubblicazione sul sito istituzionale di Ateneo.