REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO E DEL DECRETO LEGISLATIVO 30 GIUGNO 2016, 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) 27 aprile 2016, n. 679 (di seguito Regolamento UE) e del D. Lgs. n. 196/2003 come novellato dal D. Lgs. n. 101/2018 (di seguito Codice in materia di protezione dei dati personali), disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi all'interno dell'**Università degli Studi di Modena e Reggio Emilia**.
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 prevista dall'art. 6, par. 1, lett. b), e), f) del Regolamento UE.
5. L'Università considera il trattamento lecito, corretto e trasparente dei dati personali una 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 secondo la politica di protezione dei dati personali stabilita dal 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. **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;

3. **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;
4. **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;
5. **dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
6. **dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
7. **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;
8. **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;
9. **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: il direttore generale, per i dati relativi alle proprie attività, e i dirigenti delle direzioni e dell'avvocatura per le attività di propria competenza;
   - per le strutture didattiche e di ricerca: i direttori dei dipartimenti di didattica e di ricerca e dei centri, i presidenti delle scuole, i responsabili di altre tipologie di strutture;
10. **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);
11. **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);
12. **gruppo Sicurezza ICT:** l'insieme delle figure istituzionali preposte alla sicurezza di rete e sistemi quali DPO, Responsabile della transizione al digitale, APM della rete Unimore, Responsabile Servizi Informatici Reti e Sistemi, Responsabile Adeguamento GDPR, Responsabile adeguamento alle Misure Minime di Sicurezza (queste ultime due figure, così come istituite in applicazione delle direttive CAD/Agid dal progetto "Transizione al digitale" approvato dal CdA Unimore in data 21/12/2018)

13. **referenti informatici di struttura**: referenti individuati da ciascun dipartimento, direzione o altra struttura prevista nel modello organizzativo cui è affidato il compito della gestione locale dei sistemi e della rete;
14. **autorizzati al trattamento**: le persone fisiche formalmente autorizzate a istruite a trattare i dati personali sotto l'autorità diretta del Titolare e/o del Responsabile interno e per le finalità stabilite dal Titolare (artt. 4, 29, 32, 39 del regolamento UE);
15. **interessato al trattamento**: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
16. **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;
17. **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;
18. **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;
19. **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;
20. **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;
21. **limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
22. **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;
23. **responsabile per la protezione dei dati**: figura specializzata nel supporto al Titolare del trattamento prevista come obbligatoria negli enti pubblici;
24. **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
25. **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.

26. **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;
27. **stabilimento principale**: come definito dall'art. 4, par. 16 e dai Considerando 36 e 37 del Regolamento UE 679/2016. 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;
28. **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;
29. **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;
30. **gruppo imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
31. **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;
32. **autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51: per l'Italia il Garante per la protezione dei dati personali;
33. **trattamento transfrontaliero**: trattamento di dati personali che ha luogo nell'ambito dell'attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro
34. **autorità di controllo interessata**: 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; oppure c) un reclamo è stato proposto a tale autorità di controllo;
35. **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; 36. 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.

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, 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 (responsabilizzazione).

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, par. 1 del Regolamento UE.
2. 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'UNIVERSITA'

1. L'accesso ai dati interni da parte delle strutture e dei dipendenti dell'Università è ispirato al principio della libera circolazione delle informazioni all'interno dell'Università e finalizzato al raggiungimento dei fini istituzionali.
2. L'Università provvede all'organizzazione 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 da parte delle strutture o dei dipendenti dell'Università, connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, è soddisfatto in via diretta e senza ulteriori formalità nella misura necessaria al perseguimento dell'interesse istituzionale, ferma restando la responsabilità del richiedente derivante dall'utilizzo improprio dei dati.

ARTICOLO 6
TIPOLOGIE DI DATI TRATTATI DALL'UNIVERSITA'

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 Codice in materia di protezione dei dati personali, dal REGOLAMENTO UE, e dalle Linee guida e dai provvedimenti del Garante per la protezione dei dati personali.
2. L'Università effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

a) Dati, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, ivi compresi i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nell'Università:

- prove concorsuali/selezioni;
- gestione del rapporto di lavoro;
- formazione e aggiornamento professionale;
- gestione di progetti di ricerca;
- monitoraggio e valutazione della ricerca;
- attività di trasferimento tecnologico;
- politiche Welfare e per la fruizione di agevolazioni;
- salute e la sicurezza delle persone nei luoghi di lavoro;
- erogazione del servizio di telefonia fissa e mobile.

b) Dati relativi a studenti intesi nell'accezione più ampia, per tutte le attività e modalità connesse alla qualità di studente e ai laureati:

- attività di orientamento;
- erogazione dei test di ingresso o alla verifica dei requisiti di accesso;
- erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea);
- attività di tirocinio;
- attività di job placement;
- attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community;
- rilevazioni statistiche e valutazione della didattica;
- diffusione dell'elaborato finale o di elementi ad esso connessi;
- servizi di tutorato, assistenza, inclusione sociale;
- servizi e attività per il diritto allo studio;
- procedimenti di natura disciplinare a carico di studenti.

c) Dati relativi alla didattica e alla ricerca (compresa la ricerca in ambito medico - sanitario).

d) Dati relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali: - gestione degli spazi; - gestione delle postazioni; - gestione degli organi e delle cariche istituzionali; - gestione degli infortuni; - servizi bibliotecari; - servizi di protocollo e conservazione documentale; - acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso; - servizi di posta elettronica e strumenti di collaboration; - erogazione federata di servizi; - erogazione del servizio Eduroam; - accesso a servizi federati; - tracciamento di informazioni non primarie. 3. È compito dei Responsabili interni o loro Referenti effettuare e documentare la ricognizione periodica dei trattamenti.

ARTICOLO 7
TITOLARE DEL TRATTAMENTO DEI DATI

1. Il Titolare del trattamento dei dati è l'Università nel suo complesso il cui rappresentante legale è il Rettore pro tempore.
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 dette misure sono periodicamente riesaminate e aggiornate.
3. Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale l'Università è responsabile del rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal REGOLAMENTO (UE).
4. L'Università coopera con il Garante per la protezione dei 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 determinano in modo trasparente, mediante un accordo interno, i rispettivi obblighi in merito all'osservanza del Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni richieste dall'Informativa privacy, salvo quanto previsto dall'art. 26 del REGOLAMENTO (UE).
3. L' accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
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 nomina un Responsabile della protezione dei dati (di seguito RPD).
2. Il RPD è figura specializzata nel supporto al Titolare 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 l'osservanza del presente Regolamento e di altre disposizioni derivanti dalla normativa comunitaria e nazionale, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
   d) cooperare con il Garante per la protezione dei dati personali;
   e) 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;
   f) collaborare nella redazione e aggiornamento dei Registri di trattamento;
   g) svolgere ogni ulteriore compito attribuito dal Titolare.
7. 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.

8. Al RPD sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione. È garantita, inoltre, una formazione permanente per permettergli l'aggiornamento costante sugli sviluppi nel settore della protezione dei dati.
9. Il RPD ha ampio accesso alle informazioni ed è interpellato per ogni problematica inerente la protezione dei dati e per ogni attività che implica un trattamento dati, fin dalla sua progettazione.
10. L'Università garantisce che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o conflitto di interesse.
11. Il RPD non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del Regolamento UE.
12. L'Università non rimuove o penalizza il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.
13. 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 inseriti nelle informative privacy e pubblicati sul sito internet istituzionale.
14. L'amministrazione costituisce a supporto del RPD una rete di Referenti che dovranno collaborare funzionalmente con il RPD, nell'ambito delle strutture nelle quali i dati personali sono gestiti per le finalità istituzionali e sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.
15. Su indicazione del RPD possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali. 16. Il RPD redige una relazione annuale dell'attività svolta.

ARTICOLO 10
RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI

1. É Responsabile esterno del trattamento qualunque soggetto esterno che esegue, 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. I Responsabili esterni del trattamento sono nominati con atto giuridico conforme al diritto nazionale e forniscono garanzie ai sensi del paragrafo 3 dell'art. 28 del Regolamento UE, in particolare per quel che riguarda le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste dallo stesso Regolamento.
3. Il Responsabile esterno può nominare mediante contratto o altro atto giuridico subresponsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che lo legano all'Università.
4. 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 dell'altro responsabile.
5. Il Responsabile esterno risponde dinanzi all'Università dell'inadempimento del subresponsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.
6. Nell'informativa all'interessato sono indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro 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 funzione organizzativa o carica istituzionale che ricoprono, i Responsabili delle strutture nell'ambito della quale i dati personali sono gestiti per le finalità istituzionali.
2. I Responsabili interni sono così individuati: - per le attività di competenza del Rettorato: il Rettore o un suo delegato espressamente designato; - per le strutture amministrative e gestionali: il direttore generale per le attività di competenza della direzione generale e i dirigenti delle direzioni per le rispettive attività di competenza; - per le attività di didattica e di ricerca: i direttori dei dipartimenti di didattica e di ricerca e dei centri, i presidenti delle scuole, i responsabili di altre tipologie di strutture.
3. Il Responsabile interno può delegare a un proprio Referente strutturato, docente o tecnico amministrativo, i compiti di cui al successivo comma relativamente ai diversi ambiti di competenza. La delega è formalizzata con apposito atto, contiene puntualmente i compiti delegati ed è corredato dalle relative istruzioni e dalla individuazione delle modalità di verifica e di controllo. Di tale delega è data comunicazione al Rettore e al Responsabile della Protezione dei Dati, evidenza nel Registro dei trattamenti e ampia diffusione all'interno dell'amministrazione (rete intranet, ufficio personale ecc.).
4. Il Responsabile interno o suo Referente, opportunamente formato riguardo alle competenze anche decisionali in materia di protezione 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:
   - vigilare, monitorare e garantire il rispetto di quanto previsto dalle norme vigenti in materia di protezione dei dati personali;
   - rispettare ed applicare le disposizioni previste dal presente Regolamento;
   - aggiornare l'informativa privacy e la relativa modulistica;
   - collaborare, per la parte di propria competenza, nella mappatura dei trattamenti, nel censimento delle banche dati e dei trattamenti di dati esternalizzati e nella implementazione e aggiornamento del registro dei trattamenti;
   - impartire idonee istruzioni in materia di informativa privacy e di misure di sicurezza al personale autorizzato al trattamento;
   - vigilare sul rispetto delle misure di sicurezza finalizzate ad evitare i rischi, anche accidentali, di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - assicurare il costante monitoraggio degli adempimenti e delle attività effettuati dai soggetti autorizzati con particolare riferimento alla gestione della comunicazione delle violazioni di dati "data breach" e alla valutazione d'impatto privacy;
   - designare per la propria struttura i soggetti autorizzati, come definiti dall'art. 12 e verificare periodicamente i relativi livelli di autorizzazione;
   - conservare e aggiornare l'elenco dei soggetti autorizzati;
   - fornire un riscontro tempestivo, per i trattamenti di competenza, nel caso di richieste di esercizio dei diritti sui dati, così come previsto dagli artt.15-22 del Regolamento UE;
   - garantire l'esecuzione di ogni altra operazione richiesta o necessaria per ottemperare agli obblighi derivanti dalle disposizioni di legge e/o da regolamenti vigenti in materia di

protezione dei dati personali e collaborare con l'ufficio preposto per individuare i bisogni formativi delle risorse della propria struttura;
- partecipare obbligatoriamente alle sessioni informative/formative e di sensibilizzazione in materia di protezione dei dati personali; - segnalare al Titolare del trattamento e al RPD ogni variazione organizzativa che può avere un impatto sulle modalità di trattamento dei dati;
- per i trattamenti che hanno come base giuridica il consenso, predisporre le misure organizzative atte a garantire la conservazione della copia del consenso acquisito, sia esso cartaceo o elettronico, da parte della struttura autorizzata al trattamento;
- conservare, per quanto di propria competenza, e rendere disponibile su richiesta del Titolare o del RPD copia della seguente documentazione: - Accordi stipulati con i Responsabili esterni - Report delle Valutazioni di impatto Privacy (DPIA) - Valutazioni dei trattamenti basati sul legittimo interesse - Comunicazioni delle violazioni di dati personali (data breach) - Informative agli interessati relative ai trattamenti effettuati.

ARTICOLO 12
AUTORIZZATI AL TRATTAMENTO

1. Gli autorizzati al trattamento sono formalmente designati dal Responsabile interno, o suo Referente, tra il personale docente o tecnico amministrativo e operano sotto la sua diretta autorità.
2. Gli autorizzati al trattamento ricevono opportuna formazione/informazione specifica in materia di trattamento dati.
3. In assenza di formale designazione con nomina individuale di autorizzati al trattamento, coloro che trattano dati che competono alla unità organizzativa cui afferiscono, sono ritenuti autorizzati al trattamento dei dati per documentata preposizione ad unità organizzativa e pertanto sono obbligati ad osservare quanto previsto dal presente articolo.
4. L'autorizzato effettua i trattamenti dei dati personali in osservanza delle misure di sicurezza previste dall'Università, finalizzate ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati personali.
5. L'autorizzato è tenuto:
   - a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante l'attività prestata;
   - a non comunicare a terzi o diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di autorizzato;
   - a seguire i seminari d'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 eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante privacy e ai soggetti interessati (istituto del data breach).
6. L'autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici aziendali per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari, oltre che esporre l'amministrazione a danni reputazionali.

7. L’autorizzato si impegna a osservare le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica e logica adottate dall’Università.
8. Nel caso in cui non ricorrano le condizioni di cui al presente articolo, coloro che, nello svolgimento dei propri compiti, vengano a conoscenza di dati personali per i quali non possiedono esplicita autorizzazione al trattamento o che non competono alla unità organizzativa cui afferiscono, sono considerati come terzi rispetto all’amministrazione stessa, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.

ARTICOLO 13
SENSIBILIZZAZIONE E FORMAZIONE

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, l’Università sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo l’Università promuove l'attività formativa del personale universitario e l'attività informativa diretta a tutti coloro che hanno rapporti con l’Università.
2. L’Università predispone ogni anno, sentito il RPD, 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, sentito il RPCT, è integrata e coordinata con la formazione in materia di prevenzione della corruzione nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l’Università.
3. Ogni sessione formativa prevede, nell’ottica della responsabilizzazione, una prova finale di apprendimento.
4. La frequenza delle attività di formazione è obbligatoria e viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

ARTICOLO 14
INFORMATIVA

1. Per ogni tipologia di trattamento dei dati l’Università fornisce l’informativa all’interessato, salvo il caso in cui l’interessato sia già in possesso delle informazioni (art. 13, par. 4 del Regolamento UE) o in altri casi particolari previsti dall’art. 14, par. 5 del Regolamento UE. L’informativa fornita all’interessato deve essere concisa, trasparente, intellegibile, facilmente accessibile e usare un linguaggio chiaro e semplice.
2. L’informativa deve contenere:
   - 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. 4;

- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventuale volontà dell'Università di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di un fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
- il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;
- i diritti che l'interessato può esercitare, quali: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione, il diritto alla portabilità dei dati, la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, il diritto di proporre reclamo al Garante per la protezione dei dati personali;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione 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 debbano essere trattati per una finalità diversa da quella per cui sono stati raccolti, l'Università fornisce all'interessato informazioni in merito alla diversa finalità prima di tale ulteriore trattamento.
4. Nel caso in cui i dati non siano raccolti presso l'interessato, l'Università si riserva la possibilità di non fornire l'informativa nel caso in cui l'interessato già disponga delle informazioni oppure comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.
5. L'informativa può non essere fornita nel caso in cui si prefiguri il rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.
6. Le informative di competenza delle strutture sono aggiornate dai Responsabili interni o loro Referenti.
7. La modulistica, sia cartacea che digitale, che prevede la raccolta di dati riferiti a una persona fisica deve contenere almeno le seguenti informazioni:
   - la finalità per cui i dati sono raccolti e per la quale saranno usati;
   - l'indicazione di chi tratterà i dati all'interno dell'Università e se essi saranno resi disponibili a terzi;
   - l'espressione del consenso ove questo fosse una condizione di liceità del trattamento.
8. 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. I dati personali non possono essere usati per finalità diverse da quelle per le quali sono stati raccolti. Se si rendesse necessario modificare le finalità del trattamento, l'interessato dovrà essere informato della nuova finalità prima dell'inizio di qualunque trattamento. Fanno eccezione a questa disposizione i trattamenti effettuati per finalità di ricerca.

ARTICOLO 15
DIRITTI DELL'INTERESSATO

1. L'Università garantisce il rispetto dei diritti degli interessati di cui agli artt. da 12 a 22 del REGOLAMENTO UE. In particolare, l'interessato può:
   a) ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
   b) ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento;
   c) esercitare il diritto alla limitazione del trattamento non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, o dell'accertamento dei diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante;
   d) esercitare il diritto di opposizione alla profilazione;
   e) esercitare il diritto alla portabilità dei dati solo qualora il trattamento si basi sul consenso ai sensi dell'art. 6. par. 1, lettera a), o dell'art. 9, par. 2, lettera a) del Regolamento UE o su un contratto ai sensi dell'art. 6, par. 1, lettera b) del Regolamento UE e sia effettuato con mezzi automatizzati. Tale diritto non si applica al trattamento necessario per l'esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Università.
   f) esercitare il diritto all'oblio chiedendo la cancellazione dei propri dati personali nel caso questi siano stati resi pubblici on-line. Tale diritto può essere esercitato ove ricorra una delle seguenti fattispecie:
      I. i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
      II. l'interessato revoca il consenso su cui si basa il trattamento;
      III. l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
      IV. i dati personali sono trattati illecitamente;
      V. adempimento a un obbligo legale;
      VI. i dati riguardino minori.
2. L'Università informa della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione.
3. L'interessato può esercitare i suoi diritti con richiesta scritta indirizzata al Responsabile della struttura competente per la gestione dei dati personali oggetto della richiesta e in alternativa al Responsabile interno o suo Referente.
4. Il riscontro alla richiesta presentata dall'interessato viene fornito dal Responsabile dei dati di che trattasi, senza ingiustificato ritardo 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 esteso fino a 3 mesi, non ulteriormente prorogabili. Di tale proroga viene data informazione all'interessato entro un mese dalla acquisizione della richiesta al Protocollo.
5. Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.
6. 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.
7. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.
8. 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 richiesta. Il Consiglio di amministrazione stabilisce i criteri per la definizione delle modalità di pagamento e dell'importo del contributo spese da parte degli interessati.

9. La modulistica per l'esercizio dei sopra citati diritti è redatta e aggiornata a cura dei Responsabili interni o loro Referenti che devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi, nei casi più complessi, del supporto del RPD.
10. Le richieste di esercizio di diritti da parte degli interessati sono inserite all'interno di un Registro entro e non oltre 30 giorni dalla data di conclusione del procedimento.
11. Nei casi di trattamenti di dati esternalizzati, il Responsabile esterno è tenuto a collaborare con l'Università.

ARTICOLO 16
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

1. È vietato trattare 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, ai sensi dell'art. 20;

   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 ai sensi dell'art. 2-sexies del Codice in materia di protezione dei dati personali.
2. I dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento solo in conformità alle misure di garanzia disposte e adottate con apposito provvedimento dal Garante per la protezione dei dati personali.

ARTICOLO 17
TRATTAMENTO DI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

1. Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, ai sensi dell'art. 2-octies del Codice in materia di protezione dei dati personali.

ARTICOLO 18
ACCESSO AI DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO

1. I limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e per l'esercizio dell'accesso civico restano disciplinati rispettivamente dalla legge 7 agosto 1990, n. 241 e successive modificazioni e dal decreto legislativo 14 marzo 2013, n. 33 e successive modificazioni e dai Regolamenti attuativi di Ateneo in materia.
2. Quando il trattamento riguarda categorie particolari di dati personali come elencate all'art. 17, l'accesso è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

ARTICOLO 19
COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI

1. La comunicazione e la diffusione dei dati personali, esclusi i dati relativi a origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, 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, sono permesse quando:
    a. siano previste da norme di legge, di regolamento o dal diritto dell'Unione europea;
    b. siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o aggregati;
    c. siano richieste per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia;
    d. siano necessarie per il soddisfacimento di richieste di accesso ai sensi dell'art. 18.
2. La comunicazione di dati a soggetti pubblici è sempre ammessa per i fini istituzionali e ove prevista da norma di legge o regolamento.
3. Le richieste da parte di soggetti privati ed enti pubblici economici volte ad ottenere la comunicazione di dati, devono essere formulate per iscritto e motivate e devono contenere:
    - il nome, la denominazione o la ragione sociale del richiedente;
    - l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.
4. L'Università, nella figura del Responsabile interno o suo Referente, valuta, sulla base di quanto disposto dalle norme vigenti in materia di protezione dei dati personali e di quanto previsto dal presente Regolamento, eventuali richieste di comunicazione o diffusione di dati personali a soggetti privati e decide in ordine all'opportunità di effettuare la comunicazione.
5. Le modalità di comunicazione dei predetti dati, per la quale può essere richiesto un contributo a copertura dei costi sostenuti, sono decise dall'Università.
6. Al fine di favorire la comunicazione istituzionale l'Università può comunicare ad altre pubbliche amministrazioni e diffondere, anche sui propri siti web, i nominativi del proprio personale e dei collaboratori, del ruolo ricoperto, dei recapiti telefonici e degli indirizzi telematici istituzionali.

7. L'Università può comunicare a enti pubblici e privati i dati necessari alla gestione del rapporto di lavoro, relativi al personale trasferito, comandato, distaccato o comunque assegnato in servizio a un ente diverso da quello di appartenenza.
8. 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 comunicare o diffondere, anche su richiesta di soggetti privati e per via telematica, 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. La finalità deve essere dichiarata nella richiesta e i dati potranno essere utilizzati per le sole finalità per le quali sono stati comunicati e diffusi. Resta fermo il diritto dello studente alla riservatezza di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249.
9. 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.
10. 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.
11. L'Università può comunicare, alle Aziende Ospedaliere in convenzione, dati inerenti al personale dell'Università che eserciti la propria attività nell'ambito della convenzione con tali Enti.

ARTICOLO 20
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. Il trattamento dei dati relativi ai dipendenti da parte dell'Università non richiede il consenso esplicito in quanto 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.
3. L'Università garantisce ai dipendenti l'esercizio dei diritti previsti dagli articoli da12 a 22 del Regolamento UE, compreso il diritto di accesso ai dati valutativi di natura soggettiva, nonché il diritto all'informativa.
4. 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.
5. 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.
6. L'Università comunica i dati del personale addetto alla sicurezza sui luoghi di lavoro a soggetti pubblici e privati che contribuiscono alla formazione su tali tematiche.

7. 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.
8. Non è dovuto il consenso al trattamento dei dati personali presenti nei curricula 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 21
COMUNICAZIONE E DIFFUSIONE DEI DATI RELATIVI AD ATTIVITA' 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 comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei dati di cui agli articoli 17 e 18.
2. I dati di cui al precedente articolo 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 22
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 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. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a tre mesi.

ARTICOLO 23
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 24
TRATTAMENTO AI FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE O DI RICERCA STORICA

1. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.
2. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto del principio della minimizzazione dei dati.
3. Ove possibile e senza pregiudicare il raggiungimento delle finalità del trattamento, i dati dovranno essere trattati con misure tecniche che non consentano più di identificare l'interessato.
4. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità secondo i principi stabiliti dall'articolo 5 del Regolamento UE.
5. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto delle regole deontologiche in materia approvate dal Garante per la protezione dei dati personali. 6. 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 e dai Regolamenti di Ateneo in materia.

ARTICOLO 25
TRATTAMENTO AI FINI STATISTICI O DI RICERCA SCIENTIFICA

1. Il trattamento di dati personali ai fini statistici o di ricerca scientifica da parte di chiunque operi all'interno di uffici e strutture dell'Università o per conto dell'Università stessa, deve avvenire nel rispetto dei seguenti principi:

a) i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né trattati per altri scopi;

b) all'interessato deve essere fornita puntuale informazione relativamente alle finalità statistiche o di ricerca scientifica del trattamento ai sensi dell'art. 14, a meno che questo non richieda uno sforzo sproporzionato rispetto al diritto tutelato e sempre che siano adottate le idonee forme di pubblicità individuate dalle regole deontologiche in materia, promosse dal Garante.

2. Fuori dei casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di categorie particolari di dati personali, quando richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-septies del Codice in materia di protezione dei dati personali.

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 decreto legislativo 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 un livello di sicurezza adeguato al probabile rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati personali.

2. Nel valutare l'adeguato livello di sicurezza, l'Università tiene conto dei rischi che derivano in particolare 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, per il tramite del **Gruppo Sicurezza ICT** effettua la valutazione dei rischi connessi al trattamento e propone l'adozione di linee guida, se del caso, e adeguate misure di sicurezza quali, ad esempio
   - 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 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. Le misure tecniche sono riesaminate in modo periodico anche tramite audit dal Gruppo Sicurezza ICT, sono pubblicate sulla rete intranet e sono illustrate nelle sessioni formative.
5. L'Università considera rischioso il trasporto di dati personali su ogni supporto (computer portatili, copie cartacee, pendrive ecc.). Ciò vale prioritariamente per le categorie particolari di dati, i grandi volumi di dati personali e le informazioni che comportano particolari rischi per l'interessato nel caso di perdita o distruzione. Solo in circostanze eccezionali tali dati possono essere trasportati fuori dagli ambienti dell'Università e sotto la diretta responsabilità di personale autorizzato. In particolare, il personale autorizzato è tenuto a:
   - ove possibile fare uso di accesso remoto tramite login e password alle informazioni;
   - trasportare solo la quantità minima di dati personali;
   - assicurarsi che i dispositivi mobili e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali fuori dagli ambienti universitari siano dotati di sistemi di crittografia.
6. Qualunque perdita e/o furto di dati deve essere tempestivamente segnalato e trattato secondo la procedura di gestione delle violazioni di dati personali di cui all'art. 30.
7. Per quanto non espressamente disciplinato dal presente articolo sulla sicurezza, si fa rinvio a quanto disposto dai regolamenti di Ateneo di settore, in particolare quelli emanati in adempimento a quanto previsto dalle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte da AgID, Agenzia per l'Italia Digitale.

ARTICOLO 28
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

1. L'Università istituisce e aggiorna un Registro delle attività di trattamento svolte sotto la propria responsabilità.
2. Il Registro censisce le attività di trattamento svolte dagli uffici e dalle strutture dell'Università e le principali caratteristiche dei trattamenti. Il registro è costantemente aggiornato, pubblicato nella rete intranet di Ateneo e, su richiesta, messo a disposizione del Garante per la protezione dei dati personali.
3. Nel Registro sono elencati e descritti sia i trattamenti dei quali l'Università è Titolare sia i trattamenti che l'Università effettua in qualità di Responsabile esterno di altri titolari.

a) Il Registro dei trattamenti dei quali l'Università è Titolare contiene le seguenti informazioni:
- il nome ed i dati di contatto dell'Università, del RPD, dei Responsabili interni e dei loro Referenti; - le strutture competenti al trattamento; - 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;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

b) Il Registro dei trattamenti svolti dall'Università per conto di altri Titolari e per i quali l'Università si configura come Responsabile contiene le seguenti informazioni:
- il nome ed i dati di contatto dell'Università e 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;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

ARTICOLO 29
LA VALUTAZIONE DI IMPATTO PRIVACY

1. Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Responsabile interno o suo Referente, 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 su dette 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.

4. Il Responsabile interno o suo Referente si consulta con il RPD anche per assumere la decisione di effettuare o meno la valutazione di impatto. Tale consultazione e le conseguenti decisioni assunte dal Responsabile interno o suo Referente devono essere documentate nell'ambito della valutazione di impatto. Il Responsabile interno o suo Referente è tenuto a documentare le motivazioni nel caso adotti condotte difformi da quelle raccomandate dal RPD.
5. Il Responsabile per la Sicurezza e per la transizione al digitale fornisce supporto ai Responsabili interni o loro Referenti e al RPD per lo svolgimento della valutazione di impatto privacy.
6. 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.
7. L'Università, per il tramite del RPD, consulta il Garante per la Protezione dei dati personali anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica. In particolare, la consultazione è obbligatoria ove non sia necessario il consenso per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

ARTICOLO 30
VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

1. Si intende per violazione dei dati personali 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.
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, notificare la violazione di dati personali al Garante nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche, comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio sia elevato.
5. La procedura è approvata dal Consiglio di Amministrazione ed è resa disponibile attraverso la rete intranet di Ateneo.
6. La procedura costituisce una delle materie oggetto della formazione del personale di cui all'art 13.
7. Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa può comportare 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. Il trattamento dei dati personali effettuato mediante l'attivazione di impianti di videosorveglianza negli ambienti dell'Università si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.
2. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nella regolamentazione di Ateneo in materia di videosorveglianza e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria.
3. L'Università garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza. In particolare:

   - tutto il personale coinvolto nelle operazioni di registrazione, visualizzazione e registrazione delle immagini, nonché il personale addetto alla manutenzione degli impianti e alla pulizia dei locali riceve una adeguata formazione sui comportamenti da adottare in armonia con quanto previsto dalla normativa vigente in tema di protezione dei dati personali; - solo il personale autorizzato può avere accesso alle immagini;
   - il personale autorizzato è tenuto al segreto professionale;
   - le immagini non possono essere conservate per un periodo più lungo del necessario in conformità con quanto previsto dai principi applicabili al trattamento dei dati personali.
   - nel caso in cui le immagini siano conservate per un periodo maggiore di quello previsto dall'apposito regolamento, esse devono essere custodite in un posto sicuro con accesso controllato e cancellate non appena la loro conservazione non sia più necessaria.
   - è onere del Responsabile della struttura nella quale sono installati strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio:

   a) adottare le garanzie di cui all'art. 4 della legge del 20 maggio 1970, n. 300;

   b) garantire l'osservanza dei principi di necessità, finalità e proporzionalità del trattamento dei dati;

   c) garantire il rispetto del presente Regolamento, delle prescrizioni imposte dal Garante e dalla normativa vigente, anche in relazione all'utilizzo di particolari tecnologie e/o apparecchiature;

   d) redigere un documento in cui siano riportate le ragioni dell'installazione di tali sistemi anche ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso.
4. Resta ferma la necessità di effettuare una valutazione di impatto (DPIA), ai sensi dell'art. 27, comma 3, lettera c), ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.

5. Non è consentito, nel pieno rispetto dello Statuto dei lavoratori, l'uso di impianti e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

ARTICOLO 32
SANZIONI AMMINISTRATIVE

1. Fermo restando quanto previsto dagli articoli 58, 82, 83 e 84 del Regolamento UE e dal 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 CCNNLL, 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 dei componenti degli Organi per le finalità deliberative di competenza degli stessi.

ARTICOLO 34
DISPOSIZIONI FINALI

1. Il presente Regolamento, acquisito il parere del Consiglio di Amministrazione è approvato dal Senato Accademico ed emanato con Decreto Rettorale.
2. Dalla data di entrata in vigore del presente Regolamento, devono intendersi abrogate tutte le norme regolamentari e statutarie incompatibili in relazione a soggetti e materie interessate al trattamento.
3. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento (UE) 2016/679 e del D. Lgs. 196/2013 Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dal Garante.
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 PUBBLICITA'

1. Il presente Regolamento entra in vigore il giorno successivo alla sua pubblicazione sul sito web di Ateneo e alla sua affissione all'albo on line.
2. L'Università provvede a dare pubblicità al presente Regolamento ed alle successive modifiche ed integrazioni mediante pubblicazione sul Bollettino ufficiale di Ateneo e mediante diffusione interna tramite le liste di distribuzione istituzionali.

UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

Procedura di gestione della violazione dei dati personali

Data Breach Policy

Art. 30 del Regolamento in materia di protezione dei dati personali “GDPR”

Versione 1.0 del 22 Marzo 2019
Versione 2.0 del 21 Giugno 2024

Sommario

1 - Introduzione

Per violazione di dati personali deve intendersi ogni infrazione alla 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 dall'Università degli studi di Modena e Reggio Emilia.

In particolare, le tipologie di violazioni declinate dalla norma sono sintetizzabili come:

- Violazione della riservatezza che si verifica in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione dell'integrità che si verifica in caso di alterazione non autorizzata o accidentale dei dati personali;
- Violazione della disponibilità che si verifica in caso di perdita o distruzione di dati personali accidentale o illecita o di impossibilità di accesso ai dati personali da parte dei soggetti autorizzati.

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste. Lo scopo di questo documento è disegnare un flusso di procedure e di comunicazioni per la gestione delle anzidette violazioni, anche alla luce di quanto definito nella Procedura "POL01 GESTIONE DEGLI INCIDENTI DI SICUREZZA".

La presente policy è rivolta a tutti coloro che, in Ateneo, trattano a qualsiasi titolo dati personali, quindi:

- i lavoratori dipendenti ed il personale che, a prescindere dal tipo di rapporto contrattuale in essere, ha accesso ai dati personali trattati nel corso di prestazioni richieste per conto dell'Ateneo;
- qualsiasi soggetto, persona fisica o persona giuridica, che, in ragione del rapporto contrattuale in essere con l'Ateneo, abbia accesso ai dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare.

Il rispetto delle procedure è obbligatorio per tutti i soggetti coinvolti.

2 – Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato").

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione

mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Interessato: persona fisica identificata o identificabile al quale si riferiscono i dati personali. 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.

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.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, o altro organismo che tratta dati personali per conto del titolare del trattamento.

Data Protection Officer (DPO): il soggetto fisico o giuridico individuato come Responsabile della protezione dei dati personali ai sensi del GDPR.

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento o del responsabile del trattamento, con specifiche mansioni e funzioni connesse al trattamento dei dati personali.

3 - Titolare del trattamento

Il Titolare del trattamento dati (o Titolare) è l'Università degli studi di Modena e Reggio Emilia. Si evidenzia che, nell'adempimento di attività istituzionali, l'Università degli Studi di Modena e Reggio Emilia, può essere nominata **Responsabile del trattamento** in virtù di idoneo atto di nomina. La presente Procedura è applicabile anche ai trattamenti realizzati in qualità di Responsabile del trattamento.

4 - Responsabile della protezione dei dati

Il Responsabile per la Protezione dei Dati (o DPO) nominato dall'Ateneo è reperibile agli indirizzi e-mail: dpo@unimore.it, dpo@pec.unimore.it

5 - Recapito per la segnalazione della violazione

Ogni violazione deve essere prontamente segnalata all’indirizzo segnalazioni.privacy@unimore.it

6 - Procedura di gestione

La gestione di una violazione dei dati personali prevede le seguenti fasi:

1. Rilevazione e segnalazione della violazione. In particolare, tale fase può svilupparsi secondo due canali alternativi:
    A. Rilevazione e segnalazione da parte di: personale, collaboratori, studenti, fornitori o chiunque venga a conoscenza di una possibile violazione dei dati personali propri o altrui;
    B. Rilevazione e segnalazione da parte del CSIRT.
2. Raccolta informazioni e comunicazione della violazione;
3. Contenimento, recovery e risk assessment;
4. Notifica all'Autorità Garante (solo se necessaria);
5. Comunicazione agli interessati coinvolti (solo se necessaria);
6. Documentazione della violazione (Registro dei Data Breach).

Le singole fasi sono meglio descritte nei seguenti paragrafi.

6.1.A - Rilevazione e segnalazione della violazione

Chi può segnalare
Tutto il personale, i collaboratori, gli studenti, i fornitori o chiunque venga a conoscenza di una possibile violazione dei dati personali propri o altrui.
A chi segnalare
Al Responsabile della Struttura o al Referente Informatico della Struttura
Quando
Appena se ne viene a conoscenza
Come
Utilizzando le vie più brevi (telefono, e-mail, ecc.)

6.1.B - Rilevazione e segnalazione della violazione da parte del CSIRT

L'Università ha adottato la Procedura "POL01 GESTIONE DEGLI INCIDENTI DI SICUREZZA" che prevede un ruolo centrale del Gruppo Computer Security Incident Response Team ("CSIRT") e del Gruppo ICT nella gestione degli incidenti di sicurezza.

Nello svolgimento delle proprie funzioni, il CSIRT può rilevare o può ricevere segnalazioni di incidenti di sicurezza che possono determinare una violazione di dati personali. Per tale motivo, è opportuno prevedere, nella presente procedura, un ulteriore canale di rilevazione e segnalazione (alternativo rispetto a quello descritto al precedente punto 6.1.A).

Nel solo caso descritto al presente punto, il flusso di gestione passerà dalla fase 6.1.B direttamente alla fase 6.3.

Chi può segnalare

Il Responsabile Sicurezza dopo essere stato informato dal CSIRT in merito ad una segnalazione pervenuta tramite i canali previsti dalla Procedura "POL01 GESTIONE DEGLI INCIDENTI DI SICUREZZA".

A chi segnalare

Al DPO.

Quando

Tempestivamente dopo aver ricevuto la conferma che l'incidente di sicurezza presenta profili potenzialmente rilevanti in tema di protezione dei dati personali.

Come

Scrivendo a mezzo mail all'indirizzo dpo@unimore.it. In particolare, il Responsabile Sicurezza avrà cura di:

- utilizzare la seguente dicitura come oggetto della mail "!! POTENZIALE DATA BREACH – COMUNICAZIONE GRUPPO SICUREZZA ICT",
- compilare e allegare (anche in termini approssimativi, in mancanza di una conoscenza specifica degli elementi) il modulo di raccolta informazioni (Allegato A). Inoltre, è fondamentale indicare, anche nel corpo della mail, la data in cui il Responsabile Sicurezza ha avuto conferma del coinvolgimento dei dati personali;
- mettere a disposizione un contatto telefonico affinché possa intervenire un confronto per le vie brevi nel minor tempo possibile.

6.2 - Raccolta informazioni e comunicazione della violazione

Chi deve raccogliere e comunicare
Il Responsabile della Struttura o il Referente Informatico della Struttura.
A chi inviare la comunicazione
Al DPO (*) e al Gruppo Sicurezza ICT.
Quando
Appena ricevuta la segnalazione
Come
Inoltrando il modulo di raccolta informazioni (Allegato A) debitamente compilato all'indirizzo e-mail segnalazioni.privacy@unimore.it

(*) NOTA OPERATIVA PER il DPO

Nella prassi potrebbe accadere che della potenziale violazione di dati personali sia informato il solo DPO. In tal caso, laddove ritenga che il potenziale Data Breach sia determinato da un incidente di sicurezza, il DPO dovrà informare il Gruppo ICT procedendo come segue.

I. Il DPO dovrà coinvolgere il Gruppo ICT, nella persona del Responsabile Sicurezza, condividendo tutte le informazioni ricevute;
II. In particolare, il DPO avrà cura di utilizzare la seguente dicitura come oggetto della mail "!! POTENZIALE DATA BREACH – INCIDENTE SICUREZZA COMUNICAZIONE DPO".

6.3 - Contenimento, recovery e risk assessment

Chi agisce
Il DPO, d'intesa con il Titolare, il Gruppo Sicurezza ICT e i Responsabili delle Strutture coinvolte
Destinatari
I soggetti incaricati di svolgere le attività di contenimento e recovery
Quando
Nei termini indicati nell'attività di risk assessment indicati dal DPO
Come
Valutazione dei rischi legati alla violazione accertata. Valutazione della necessità di comunicazione della violazione al Garante e agli interessati e, in caso affermativo, informazione al Titolare affinché venga inoltrata la notifica al Garante. Individuazione dei soggetti incaricati delle attività di contenimento e recovery. Definizione delle operazioni da svolgere e dei tempi di attuazione. Comunicazione delle operazioni da effettuare ai soggetti incaricati. Eventuali operazioni di verifica di efficacia delle misure di contenimento e recovery stabilite ed eventuale prosecuzione delle indagini a seguito di indicazioni da parte del Garante o del Titolare.

6.4 - Notifica all'Autorità Garante (solo se necessaria)

Chi la effettua
Il Titolare, sentito il DPO.
A chi viene inoltrata
All'Autorità di controllo, ossia il Garante per la protezione dei dati personali.
Quando
Entro 72 ore dal momento in cui il titolare del trattamento viene a conoscenza della violazione di dati personali. NB: Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, deve essere corredata dei motivi del ritardo.
Come
Mediante la modulistica e i canali di comunicazione predisposti dal Garante, reperibili sul sito istituzionale: www.gpdp.it

6.5 - Comunicazione agli interessati coinvolti (solo se necessaria)

Chi la effettua
Il Titolare, sentito il DPO.
A chi viene inoltrata
Alle persone fisiche i cui dati sono stati violati.
Quando
Nel più breve tempo possibile, senza ingiustificato ritardo.
Come
Mediante comunicazione diretta o mediante pubblicazione in sito a loro accessibile.

6.6 - Documentazione della violazione (Registro dei Data Breach)

Chi compila il documento
Il DPO insieme al responsabile della Struttura coinvolta nella violazione ovvero, se coinvolti, al CSIRT e al Gruppo ICT
Quando
Ogni volta che riceve la segnalazione di una violazione.
Come
Registrazione della violazione nel Registro dei Data Breach con la descrizione della violazione, delle azioni intraprese e annotazione dei successivi aggiornamenti se necessario proseguire le indagini. Registrazione della risposta del Garante e delle eventuali prescrizioni in essa contenute. Registrazione della chiusura dell'incidente se non necessita di ulteriori indagini oppure indicazione della prosecuzione delle indagini.

Allegato A - Modulo per la raccolta informazioni

In caso di scoperta di un data breach:

1. **Informare immediatamente il Responsabile della struttura di afferenza e/o il Referente Informatico**
2. **Il Responsabile della Struttura o il Referente Informatico devono compilare il modulo seguente e inviarlo via mail a segnalazioni.privacy@unimore.it**

Data della violazione

- ❑ tra il __ / __ / ____ e il __ / __ / ____
- ❑ in un tempo non ancora determinato
- ❑ è possibile che sia ancora in corso

Luogo della violazione[1]

Riferimenti di chi segnala la violazione [2]

Descrizione dell'evento in breve[3]

Banche dati oggetto di data breach e breve descrizione dei dati personali trattati

Tipo di violazione

- ❑ Lettura (presumibilmente i dati non sono stati copiati)
- ❑ Copia (i dati sono ancora presenti sui sistemi del Titolare)
- ❑ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ❑ Cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)
- ❑ Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)
- ❑ Altro: _____

Tipo di dati oggetto della violazione

- ❑ Dati anagrafici
- ❑ Numero di telefono (fisso o mobile)
- ❑ Indirizzo di posta elettronica
- ❑ Dati di accesso e di identificazione (user name, password, altro)
- ❑ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- ❑ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari
- ❑ Altro: _____

Dispositivo oggetto della violazione

- ❑ Computer
- ❑ Rete
- ❑ Dispositivo mobile
- ❑ File o parte di un file
- ❑ Strumento di backup
- ❑ Documento cartaceo
- ❑ Altro: _____

[1] Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili

[2] Indicare nome, cognome, e-mail, telefono se personale interno, ragione sociale se personale esterno

[3] Riportare una descrizione sintetica del data breach, dei sistemi di elaborazione o memorizzazione dei dati coinvolti, la loro ubicazione, le categorie e il numero approssimativo di persone interessate dalla violazione