UNIVERSITÀ DI PARMA

2022

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sommario

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 relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
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 del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo esterno che tratta dati personali per conto del titolare del trattamento;
9. **referente privacy:** il responsabile delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, individuato sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricopre, come definito nell'art. 10.1 del presente regolamento;
10. **delegato privacy:** figura designata dal Referente privacy per svolgere operativamente i compiti a lui assegnati e per interfacciarsi con l'RPD/DPO come definito nell'art. 10.2 del presente regolamento;
11. **responsabile scientifico:** titolari di ricerche, nell'ambito di progetti nazionali e internazionali e figure assimilate come definiti nell'art. 10.3 del presente regolamento;

12. **Team Privacy**: gruppo a supporto del DPO/RPD e di raccordo con le varie articolazioni dell'ente come definito nell'art.7 del presente regolamento;
13. **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);
14. **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);
11. **responsabile della sicurezza informatica:** responsabile dell'Unità Organizzativa che coordina le attività relative alla sicurezza IT in Ateneo;
12. **autorizzati al trattamento:** le persone fisiche formalmente autorizzate e istruite a trattare i dati personali sotto l'autorità diretta del Titolare e/o del Referente privacy e per le finalità stabilite dal Titolare (artt. 4, 29, 32, 39 del regolamento UE);
13. **interessato al trattamento:** la persona fisica a cui si riferiscono i dati personali;
14. **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;
15. **terzo:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento, il Referente privacy del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento;
16. **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;
17. **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;
18. **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;
19. **limitazione di trattamento:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
20. **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;

21. **responsabile per la protezione dei dati (RPD o Data Protection Officer DPO):** è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e di controllo, consultive, formative e informative relativamente all'applicazione del RGPD.;
22. **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 del trattamento secondo le rispettive competenze;
23. **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;
24. **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;
25. **stabilimento principale:** come definito dall'art. 4, par. 16 e dai Considerando 36 e 37 del Regolamento UE. Per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
26. **rappresentante:** la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27 del Regolamento UE, li rappresenta per quanto riguarda gli obblighi rispettivi;
27. **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;
28. **gruppo imprenditoriale:** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
29. **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;
30. **autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE: per l'Italia il Garante per la protezione dei dati personali;
31. **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;

32. **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;
33. **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;
34. **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 1 – PRINCIPI E AMBITO DI APPLICAZIONE

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 di Parma

L'Università in qualità di titolare del trattamento effettua i trattamenti di dati con o senza ausilio di processi automatizzati.

I dati sono trattati nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.

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), del Regolamento UE.

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.

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.

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

In particolare, i dati personali sono:

1. Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
2. 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;

3. Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
4. 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);
5. 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);
6. 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).

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 2 - BASE GIURIDICA DEL TRATTAMENTO

L'Università è una Pubblica Amministrazione ai sensi dell'art. 1, c. 2 del D. Lgs. 165/2001 e ss.mm.ii., 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.

Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato (principio di necessità) e non deve essere lesivo dei diritti e delle libertà fondamentali delle persone fisiche (art. 1, c. 2 Regolamento UE)".

ARTICOLO 3 - CIRCOLAZIONE DEI DATI ALL'INTERNO DELL'UNIVERSITA'

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.

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.

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, previa formale richiesta che ne illustri le motivazioni, nella misura necessaria

al perseguimento dell'interesse istituzionale, ferma restando la responsabilità del richiedente derivante dall'utilizzo improprio dei dati.

ARTICOLO 4 - TIPOLOGIE DI DATI TRATTATI DALL'UNIVERSITA'

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.
L'Università effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

1. Dati, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, ivi compresi i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nell'Università:
    a. prove concorsuali/selezioni;
    b. gestione del rapporto di lavoro; formazione e aggiornamento professionale; gestione di progetti di ricerca; monitoraggio e valutazione della ricerca; attività di trasferimento tecnologico;
    c. 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.
2. Dati relativi a studenti intesi nell'accezione più ampia, per tutte le attività e modalità connesse alla condizione di studente e ai laureati:
    a. attività di orientamento;
    b. erogazione dei test di ingresso o alla verifica dei requisiti di accesso;
    c. erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea);
    d. attività di tirocinio; attività di job placement;
    e. attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community;
    f. rilevazioni statistiche e valutazione della didattica;
    g. diffusione dell'elaborato finale o di elementi ad esso connessi; servizi di tutorato, assistenza, inclusione sociale;
    h. servizi e attività per il diritto allo studio;
    i. procedimenti di natura disciplinare a carico di studenti.

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

4. Dati relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali:
    a. gestione degli spazi;
    b. gestione delle postazioni;
    c. gestione degli organi e delle cariche istituzionali;
    d. gestione degli infortuni;
    e. servizi bibliotecari;
    f. servizi di protocollo e conservazione documentale;
    g. acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del

contenzioso;

h. servizi di posta elettronica e strumenti di collaborazione;
i. erogazione federata di servizi (ad es. Eduroam);
j. tracciamento di informazioni non primarie per la corretta e completa esecuzione dei servizi offerti agli Utenti attraverso i sistemi informativi di Ateneo.

5. È compito dei Referenti privacy o loro Delegati privacy effettuare e documentare la ricognizione periodica dei trattamenti.

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

ARTICOLO 5 - TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento dei dati è l'Università nel suo complesso il cui rappresentante legale è il Rettore pro tempore.
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.
Nel caso di trasferimento di dati personali verso un Paese terzo o ad una 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.
L'Università coopera con il Garante per la protezione dei dati personali.
Il titolare, consapevole dell'importanza di adottare politiche di protezione dei dati personali trattati nell'esercizio dei propri compiti istituzionali, si impegna ad effettuare il trattamento in applicazione dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.

ARTICOLO 6 - CONTITOLARE

Quando uno o più titolari del trattamento determinano congiuntamente con l'Università le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.
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.
L' accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati, anche successivamente allo scioglimento del rapporto di contitolarità. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

L'interessato può esercitare i propri diritti nei confronti di ciascun contitolare del trattamento.

ARTICOLO 7 - IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD) O DATA PROTECTION OFFICER (DPO)

L'Università nomina un Responsabile della protezione dei dati (di seguito RPD/DPO).
Il RPD/DPO 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.
Il RPD/DPO 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 assegnati.
Il RPD/DPO può essere un soggetto interno (dipendente dell'Università) o esterno, assolvendo in tal caso i suoi compiti in base a un contratto di servizi.
Il RPD/DPO è nominato, nel caso di soggetti interni, con decreto del Rettore.
Il RPD/DPO è tenuto a svolgere i seguenti compiti (secondo quanto previsto dall'art. 39 del Regolamento UE):

1. informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento, dal Regolamento UE e dalla normativa comunitaria e nazionale relativa alla protezione dei dati;
2. vigilare circa l'osservanza del presente regolamento, del Regolamento UE e di altre disposizioni derivanti dalla normativa comunitaria e nazionale, compresa l'attribuzione delle responsabilità;
3. fornire indicazioni e collaborare con il Titolare circa le attività di formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
4. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
5. cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto con detta autorità per questioni connesse al trattamento, tra cui la consultazione preventiva, segnalazioni di violazione dei dati personali, cooperando con il titolare per l'eventuale presentazione delle notifiche obbligatorie di violazione dei dati personali ai sensi del Regolamento UE;
6. fornire indicazioni per la redazione e l'aggiornamento dei Registri di trattamento;
7. redigere una relazione annuale dell'attività svolta.

Per lo svolgimento dei propri compiti il RPD/DPO si avvale di un *Team privacy* composto almeno da:

- un rappresentante per ogni Area Dirigenziale e per ogni Dipartimento (delegato privacy ai sensi all'art 10.2 del presente regolamento);
- un rappresentante della UO Sicurezza IT con funzioni di coordinamento;
- un rappresentante della UO Legale e compliance.

A seconda della necessità, il RPD/DPO può avvalersi di professionalità interne od esterne all'Ateneo.
Nell'eseguire i propri compiti il RPD/DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
Il RPD/DPO ha ampio accesso alle informazioni ed è interpellato per ogni

problematica inerente alla protezione dei dati e per ogni attività che implica un trattamento dati, fin dalla sua progettazione. A tal fine il RDP/DPO deve essere invitato a partecipare alle riunioni di coordinamento dei dirigenti/responsabili/direttori di dipartimento e dei centri che abbiano per oggetto questioni inerenti alla protezione dei dati personali.
L'Università garantisce che il RPD/DPO 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.
Il RPD/DPO non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del Regolamento UE.
L'Università non rimuove o penalizza il RPD/DPO in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.
Il nominativo e i dati di contatto del RPD/DPO sono comunicati al Garante per la protezione dei dati personali. I dati di contatto del RPD/DPO sono inseriti nelle informative privacy e pubblicati sul sito internet istituzionale.
Per lo svolgimento dei compiti di cui al precedente comma 6, l'amministrazione costituisce a supporto del RPD/DPO una rete di Delegati privacy, ognuno dei quali collaborerà con RPD/DPO 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.
Al RPD/DPO sono garantite autonomia e risorse per svolgere in modo efficace i compiti attribuiti, in relazione alle dimensioni organizzative dell'ente; in particolare, sono garantite risorse per l'acquisizione di beni e/o servizi funzionali all'assolvimento dei compiti e tempi di lavoro adeguati allo svolgimento della sua funzione. È garantita inoltre, a lui e al personale che collabora con lui, una formazione permanente per permettere l'aggiornamento costante sugli sviluppi nel settore della protezione dei dati.
Su indicazione del RPD/DPO possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali e per specifiche tematiche.

ARTICOLO 8 - RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

È Responsabile 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.
I Responsabili 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.
Il Responsabile del trattamento può nominare mediante contratto o altro atto giuridico sub- responsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che lo legano all'Università.
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.

Il Responsabile del trattamento risponde dinanzi all'Università dell'inadempimento del sub- responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.
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 9 – AUTORIZZATI AL TRATTAMENTO

Sono considerati autorizzati al trattamento **tutti coloro che**, nello svolgimento delle loro mansioni, **accedono ai dati personali necessari al perseguimento delle finalità attribuite all'unità organizzativa di appartenenza**. 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.
Gli autorizzati al trattamento ricevono opportuna formazione/informazione specifica in materia di trattamento dati.
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.
L'autorizzato è tenuto:

1. 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;
2. 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 designato;
3. 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;
4. a segnalare con tempestività al proprio responsabile di ufficio e al Referente privacy eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante privacy e ai soggetti interessati (istituto del data breach).

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 anche di natura reputazionale.
L'autorizzato si impegna a osservare le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica adottati dall'Università.
Nel caso in cui non ricorrano le condizioni di cui al presente articolo, coloro che, nello svolgimento dei propri compiti, vengano accidentalmente 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 e come tali dovranno osservare il divieto alla comunicazione e all'utilizzazione dei dati, considerando illegittimo ogni loro trattamento.
Il Titolare predispone e mantiene aggiornati i documenti per stabilire gli specifici permessi di accesso ai dati di ogni singolo designato in relazione alla sua posizione nell'organigramma.

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

- effettuare ricerche per la redazione della tesi di laurea e/o altri elaborati sottoposti a valutazione didattica;
- agire in relazione ad attività funzionalmente e sostanzialmente connesse con l'attività didattica e formativa dell'Ateneo.

Se lo studente, ai fini della redazione della tesi, raccoglierà dati personali di titolarità dell'Ateneo, dovrà inoltre avere cura di somministrare agli interessati l'informativa per la raccolta dei dati, utilizzando il modello adeguato pubblicato nella sezione privacy del portale di Ateneo, compilato sulla scorta delle particolarità e dei riferimenti al trattamento da effettuare. In ogni caso, al fine di poter provare che il tesista abbia adempiuto agli obblighi di informazione e di raccolta del consenso, al momento del deposito del titolo della tesi dovrà consegnare agli uffici amministrativi a corredo della documentazione anche il modello di informativa utilizzato ed eventualmente anche i consensi raccolti se necessari.

Sono altresì da considerare autorizzati al trattamento **i tirocinanti, gli stagisti, gli studenti collaboratori 150 ore** e le figure a questi affini, che in ragione del loro status, **svolgono la loro attività all'interno dell'Ateneo**. È pertanto onere dell'Ateneo formalizzare e autorizzare il soggetto al trattamento dati in ragione dell'incarico o dell'attività che questi andrà a svolgere.

Qualora, invece, lo studente ricopra il ruolo di collaboratore, tirocinante o stagista, in un Ente terzo, in ragione di una convenzione tra questo e l'Ateneo, sarà l'Ente ospitante a dover formare lo studente al trattamento dei dati nella propria struttura. Tale aspetto dovrà essere concordato con l'Ente al momento della stipula della convenzione unitamente alla qualifica che si intende attribuire allo studente ospitato dall'Ente terzo.

ARTICOLO 10 - I DESIGNATI AL TRATTAMENTO

In Ateneo sono individuate le seguenti categorie di designati al trattamento ai sensi dell'art. 29 del Regolamento UE e dell'art. 2 quaterdecies del d.lgs 101/2018:

1. I Referenti privacy
2. I Delegati privacy
3. I Responsabili scientifici

ARTICOLO 10.1 - I REFERENTI PRIVACY

I Responsabili delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono, sono individuati quali Referenti privacy.
I Referenti privacy 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.
- in relazione ai **Centri di Servizio dei Dipartimenti**: il **Responsabile amministrativo** del Centro di Servizio o un suo delegato.

I Referenti privacy hanno il compito di coadiuvare il Titolare nella definizione delle finalità, delle modalità di trattamento e dei mezzi atti a garantire l'osservanza della normativa europea e nazionale sul trattamento dei dati personali, nonché delle relative policy interne all'Ateneo, nello svolgimento dei compiti di cui al paragrafo successivo.

Il Referente privacy collabora funzionalmente con il RPD/DPO, opera con autonomia gestionale nell'ambito delle competenze affidategli e può delegare a un proprio Delegato privacy (vedi art. 10.2 del presente regolamento) strutturato, docente o tecnico amministrativo, i compiti elencati di seguito relativamente alla propria struttura di afferenza e per gli ambiti espressamente definiti:

1. vigilare, monitorare e garantire il rispetto di quanto previsto dalle norme vigenti in materia di protezione dei dati personali;
2. rispettare ed applicare le disposizioni previste dal presente Regolamento;
3. aggiornare l'informativa privacy e la relativa modulistica;
4. collaborare, per le parti 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;
5. impartire idonee istruzioni in materia di informativa privacy e di misure di sicurezza al personale designato al trattamento;
6. 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;
7. 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;
8. 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;
9. 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;
10. partecipare obbligatoriamente alle sessioni informative/formative e di sensibilizzazione in materia di protezione dei dati personali;
11. segnalare al Titolare del trattamento e al RPD/DPO ogni variazione organizzativa che può avere un impatto sulle modalità di trattamento dei dati;
12. 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/DPO 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.

La delega è formalizzata con apposito atto, contiene i compiti delegati ed è corredato dalle relative istruzioni. Di tale delega è data comunicazione al Rettore e al Responsabile della Protezione dei Dati.

ARTICOLO 10.2 - I DELEGATI PRIVACY

Il Delegato privacy viene nominato per iscritto dal Referente privacy che gli impartisce tutte le istruzioni necessarie per lo svolgimento dei propri compiti e finalizzate al rispetto delle norme. In caso di cessazione o revoca dell'incarico, il Referente privacy comunica all'ufficio di supporto del RPD/DPO il nuovo nominativo.
L'elenco dei Referenti privacy e dei loro relativi Delegati privacy per la protezione dei dati è comunicato al Rettore e al RPD/DPO.

ARTICOLO 10.3 - I RESPONSABILI SCIENTIFICI

I Responsabili Scientifici sono i titolari di ricerche, nell'ambito di progetti nazionali e internazionali e figure assimilate.
Trattano i dati nell'ambito del proprio progetto di ricerca e sono i referenti per l'attività svolta e vigilano sul trattamento e la protezione dei dati riguardo al rispetto delle disposizioni normative comunitarie e internazionali relative al trattamento dei dati personali ai fini statistici e scientifici e conformemente alle prescrizioni e regole deontologiche adottate e approvate dal garante per la protezione dei dati.
Il Responsabile Scientifico è designato al trattamento dal Titolare quando svolge attività di ricerca propria dell'Università di Parma, anche nell'ambito di attività di ricerca nazionali e internazionali.
I soggetti appartenenti al gruppo di ricerca relativo ad un determinato studio devono essere autorizzati al trattamento dei dati dal Responsabile Scientifico stesso.

ARTICOLO 11 - AMMINISTRATORI DI SISTEMA

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

Egli risponde, inoltre, delle attività svolte e delle conseguenze derivanti da un malfunzionamento della rete e supporta Responsabili del Trattamento e Autorizzati per gli aspetti di tipo tecnico informatico nelle normali attività operative.
Il titolare del trattamento verifica la rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.

ARTICOLO 12 - SENSIBILIZZAZIONE E FORMAZIONE

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 strutta 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.
L'Università predispone ogni anno, sentito il RPD/DPO, 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. I contenuti del piano formativo tengono in considerazione le criticità emerse nell'anno precedente relativamente all'applicazione del presente regolamento, degli incidenti riguardanti la riservatezza, l'integrità e la disponibilità dei dati, il rispetto dei diritti dell'interessato e delle novità normative, giurisprudenziali e di prassi intervenute in materia di trattamento dei dati personali. Tale formazione è coordinata con la formazione in materia di sicurezza informatica.
Ogni sessione formativa prevede, nell'ottica della responsabilizzazione, una prova finale di apprendimento.
La frequenza delle attività di formazione è obbligatoria e viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

ARTICOLO 13 - INFORMATIVA

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.
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.
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.
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 nel caso in cui comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.

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.
Al fine di adempiere all'obbligo informativo, secondo i principi sopra esposti e ai fini dell'accountability, l'Università degli Studi di Parma rende disponibili modelli di informative nello spazio web dedicato alla Privacy.

ARTICOLO 14 - CONSENSO

Ai sensi dell'art. 6, paragrafo 1, lett. c), d), e) del Regolamento UE, l'Ateneo non è tenuto a richiedere il consenso al trattamento dei dati personali per tutte le finalità inerenti alle attività istituzionali dell'Università, per ottemperare ad obblighi di legge e per ragioni di pubblica sicurezza.
Per le finalità che non rientrano nelle finalità istituzionali, o per le quali il trattamento sia reso obbligatorio da previsioni di legge o da ragioni di pubblica sicurezza, dovrà essere valutata qual è la base giuridica adeguata alle specifiche finalità per le quali viene eseguito il trattamento.
Il Referente privacy e i relativi Delegati privacy definiscono la base giuridica del trattamento nell'ambito del sistema di progettazione dei trattamenti, nel rispetto dei principi di "privacy by design" e di "privacy by default".
Nel caso la base giuridica individuata fosse il consenso (art. 6, paragrafo 1 lett. a) del Regolamento UE), dovrà sempre essere prevista:

1. una modalità di raccolta del consenso idonea a poter dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
2. una modalità che permetta all'interessato di revocare il consenso in qualunque momento, con la stessa facilità con la quale è stato accordato.

ARTICOLO 15 - DIRITTI DELL'INTERESSATO

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:

1. 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;
2. ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento;
3. 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;
4. esercitare il diritto di opposizione alla profilazione;
5. 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;

6. 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:
    a. i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
    b. l'interessato revoca il consenso su cui si basa il trattamento;
    c. l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere altrattamento;
    d. i dati personali sono trattati illecitamente;
    e. adempimento a un obbligo legale;
    f. i dati riguardino minori.

L'Università informa della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione.

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 Referente privacy o suo Delegato privacy.

Il riscontro alle richieste dell'interessato è regolato da una procedura dedicata, "Procedura per la gestione dei diritti dell'interessato", nel rispetto dei seguenti principi: il riscontro viene fornito dal Referente privacy, 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.

Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.

L'Università agevola, per il tramite dei Referenti privacy o loro Delegati privacy, l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa.

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.

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.

La modulistica per l'esercizio dei sopra citati diritti è redatta e aggiornata a cura dei Referenti privacy o loro Referenti per la protezione dei dati che devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi, nei casi più complessi, del supporto del RPD/DPO.

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.

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

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, (di seguito anche solo "categorie particolari di dati personali", così come individuati dall'art. 9 Regolamento UE), fatti salvi i seguenti casi:

1. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
2. 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. 19 del presente regolamento;
3. 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;
4. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
5. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
6. 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, se previsto dal diritto dell'Unione Europea ovvero da disposizioni di legge, di regolamento o da atti amministrativi generali. Si considerano di rilevante interesse pubblico i trattamenti eseguiti nelle seguenti materie:
    - accesso a documenti amministrativi e accesso civico;
    - concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
    - rapporti tra i soggetti pubblici e gli enti del terzo settore;
    - obiezione di coscienza;
    - attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
    - rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
    - compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
    - programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
    - tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
    - istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
    - instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materiale sindacale, occupazione e collocamento obbligatorio, previdenza e

assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, tutela del patrimonio informativo dell'Ateneo, igiene e sicurezza di lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

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.

Tali dati non possono essere diffusi. E' ammesso l'utilizzo nel rispetto delle garanzie di cui all'art. 2_septies del Codice.

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

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 e Regolamento UE.

In particolare, è ammesso nei seguenti casi:

1. adempimento di obblighi ed esercizio di diritti da parte del Titolare o dell'interessato nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento;
2. adempimento di obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione di controversie civili e commerciali;
3. verifica o accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
4. accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
5. accertamento, esercizio o difesa di un diritto in sede giudiziaria;
6. esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
7. adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
8. accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
9. adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

ARTICOLO 18 - ACCESSO AI DOCUMENTI AMMINISTRATIVI E ACCESSO

CIVICO

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.
Quando il trattamento riguarda categorie particolari di dati personali, 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

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:

1. siano previste da norme di legge, o, nei casi previsti dalla legge, di regolamento o da atti amministrativi generali, ai sensi dell'art. 2-ter del Codice della Privacy, ovvero, quando è comunque necessaria per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri attribuiti all'Ateneo;
2. siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o aggregati;
3. 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;
4. siano necessarie per il soddisfacimento di richieste di accesso ai sensi dell'art. 18 del presente regolamento.

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:

1. il nome, la denominazione o la ragione sociale del richiedente;
2. l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.

L'Università, nella figura del Referente privacy o suo Delegato privacy, 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.
Le modalità di comunicazione dei predetti dati, per la quale può essere richiesto un contributo a copertura dei costi sostenuti, sono decise dall'Università.
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.

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.
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, 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.
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.
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.
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

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.
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.
L'Università garantisce ai dipendenti l'esercizio dei diritti previsti dagli articoli dal 2 a 22 del Regolamento UE, compreso il diritto di accesso ai dati valutativi di natura soggettiva, nonché il diritto all'informativa.
L'Università adotta misure tecniche e organizzative atte a garantire la tutela, adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui, ivi comprese le 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.
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 fomiti 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.
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.
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.
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

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 (con esclusione dei dati di cui agli articoli 16 e 17 del presente regolamento) relativi a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi che partecipano ad attività di studio e di ricerca.
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.
L'Università può comunicare eventuali informazioni inerenti alla 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:

1. 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;
2. 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;
3. 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.

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

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.
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.

Le valutazioni sono rese disponibili per un periodo di tempo non superiore a tre mesi.

ARTICOLO 23 - DIFFUSIONE DEI RISULTATI DI CONCORSI E SELEZIONI

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.
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.
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

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.
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.
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.
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.
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.
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

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:

1. 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;

2. all'interessato deve essere fornita puntuale informazione relativamente alle finalità statistiche o di ricerca scientifica del trattamento ai sensi dell'art. 13 del presente regolamento, 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.

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

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.

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.

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.

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

L'Università mette in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al probabile rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati personali.

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.

Ogni Referente privacy (in relazione ai trattamenti di propria competenza) prima di iniziare un nuovo trattamento o di modificare un trattamento già in essere, effettua la

valutazione dei rischi connessi al trattamento stesso e la sottopone alla valutazione dello Staff del RPD/DPO che fornisce un parere e suggerisce eventuali misure correttive.
Il Referente privacy adotta quindi le misure di sicurezza idonee a ridurre i rischi individuati. Le principali misure comprendono:

1. la pseudonimizzazione e la cifratura dei dati;
2. la minimizzazione dei dati;
3. le misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni;
4. la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico;
5. una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
6. la corretta gestione delle autorizzazioni e delle credenziali di accesso;
7. strumenti di verifica della sicurezza dei dispositivi su cui vengono trattati i dati.

Le misure tecniche sono riesaminate in modo periodico tramite audit dall'Unità Organizzativa Sicurezza IT e sono illustrate nelle sessioni formative.
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:

1. ove possibile fare uso di accesso remoto tramite login e password alle informazioni conservate su sistemi sicuri individuati dall'Ateneo;
2. trasportare solo la quantità minima di dati personali;
3. assicurarsi che i dispositivi mobili (ad es. pc portatili, tablet etc.) e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali fuori dagli ambienti universitari siano dotati di sistemi di crittografia.

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 del presente regolamento.
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 dal Documento Programmatico per la Sicurezza e dalle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte da AgID, Agenzia per l'Italia Digitale.

ARTICOLO 28 – REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'Università istituisce e aggiorna un Registro delle attività di trattamento svolte sotto la propria responsabilità.
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 gestito e aggiornato dai Referenti privacy e/o Delegati privacy e, su richiesta, messo a disposizione del Garante per la protezione dei dati personali.
A corredo del registro è archiviata e gestita dai Referenti privacy e/o Delegati privacy la documentazione a supporto delle decisioni di ogni singolo trattamento.

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.

Il Registro dei trattamenti dei quali l'Università è Titolare contiene le seguenti informazioni:

1. il nome ed i dati di contatto dell'Università, del RPD/DPO, dei Referenti privacy e dei loro Delegati privacy;
2. le strutture competenti al trattamento;
3. le finalità del trattamento;
4. le basi giuridiche del trattamento;
5. la descrizione delle categorie di interessati, nonché le categorie di dati personali;
6. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
7. l'eventuale trasferimento di dati personali verso un paese terzo o una organizzazione internazionale;
8. i criteri temporali di conservazione dei dati;
9. ove possibile il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

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:

1. il nome ed i dati di contatto dell'Università e del RPD/DPO;
2. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
3. 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;
4. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

ARTICOLO 29 – PRIVACY BY DESIGN, PRIVACY BY DEFAULT LA VALUTAZIONE DI IMPATTO PRIVACY

In occasione di cambiamenti organizzativi e tecnologici che coinvolgano il trattamento di dati personali – sia nel caso di trattamenti già in essere sia nel caso di nuovi trattamenti, come meglio descritto nei commi successivi – dovrà essere verificata l'applicazione dei principi di "privacy by design" e di "privacy by default" (ex art. 25 del Regolamento UE). Tale verifica procederà, in primis, dal considerare la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie. Lo staff del DPO mette a disposizione una specifica metodologia per effettuare la predetta analisi e la progettazione degli strumenti del trattamento. Nel caso in cui dall'analisi emerga che tali profili determinano un rischio elevato per i diritti e le libertà delle persone fisiche, prima della progettazione degli strumenti del trattamento, il Referente privacy o suo Delegato privacy, in collaborazione con lo staff del DPO e previa consultazione con il RPD/DPO, effettua, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali (ex art. 35 del Regolamento UE). La valutazione è condotta applicando una specifica procedura, adottata dallo staff del DPO, i cui risultati saranno valutati dal DPO stesso. Successivamente, la progettazione degli strumenti avverrà tenendo conto degli esiti della valutazione d'impatto. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.

In particolare, il Referente privacy o suo Delegato privacy devono tenere conto che la valutazione d'impatto sulla protezione dei dati è obbligatoria nei casi seguenti:

1. 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;
2. 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;
3. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza);
4. il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico;
5. oppure, qualora si presentino due delle condizioni individuate dalle Linee Guida del Garante europeo in merito alla valutazione d'impatto.

Il Referente privacy o suo Delegato privacy si consulta con il RPD/DPO e il suo staff anche per assumere la decisione di effettuare o meno la valutazione di impatto. Tale consultazione e le conseguenti decisioni assunte dal Referente privacy o suo Delegato privacy devono essere documentate nell'ambito della valutazione di impatto. Il Referente privacy o suo Delegato privacy, in collaborazione con lo staff del DPO è tenuto a documentare le motivazioni nel caso adotti condotte difformi da quelle raccomandate dal DPO. Nel caso in cui, successivamente allo svolgimento della DPIA, il Referente privacy ritenesse di effettuare il trattamento, nonostante il parere negativo del DPO, l'autorizzazione al trattamento dovrà essere assunta dal Titolare dei dati.

Il Responsabile per la transizione al digitale fornisce supporto ai Referenti privacy o loro Delegati privacy e al RPD/DPO per lo svolgimento della valutazione di impatto privacy.

I Delegati privacy devono collaborare nella conduzione della valutazione di impatto fornendo ogni informazione e documentazione necessaria.

L'Università, per il tramite del RPD/DPO, 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.

L'Università, per il tramite del RPD/DPO, 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)

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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la

disponibilità di dati personali.
I principali rischi per i diritti e le libertà delle persone fisiche conseguenti ad una violazione, in conformità al considerando 75 del Regolamento UE sono:

1. danni fisici, materiali o immateriali;
2. limitazioni dei diritti;
3. discriminazioni;
4. furto o usurpazione d'identità;
5. perdite finanziarie;
6. pregiudizio alla reputazione;
7. perdita di riservatezza dei dati personali protetti da segreto professionale;
8. decifratura non autorizzata della pseudonimizzazione.

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 (A*llegato Procedura gestione data breach)*.
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.
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.
La procedura è resa disponibile attraverso la rete intranet di Ateneo.
La procedura costituisce una delle materie oggetto della formazione del personale di cui all'art 12 del presente regolamento.
Chiunque venga a conoscenza, direttamente e/o indirettamente (su indicazione di un incaricato, di un dipendente dell'Ateneo e/o di un terzo) di una possibile violazione di dati personali (anche solo sospetta) – quale che sia la possibile fonte/origine di tale violazione (terzi, personale dell'Ateneo, fonte non identificata, evento accidentale) – deve comunicare immediatamente al RDP/DPO e al Referente privacy tale possibile violazione attraverso i canali indicati nella *Procedura gestione databreach*.
Il RPD/DPO chiede all'Area Sistemi Informativi un report Tecnico inerente alla violazione che deve pervenire entro 36 ore dalla richiesta sottoscritto dal Referente privacy o suo Delegato privacy. Eventuali ritardi dovranno essere motivati.
Il RPD/DPO svolge l'istruttoria sulla violazione tenendo conto del report Tecnico fornito e propone al titolare di 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 e di comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio sia elevato.
Se tecnicamente possibile, il report tecnico dovrà essere corredato dalla cristallizzazione dei dati relativi all'attacco, ove questo costituisse una violazione dei dati, allo scopo di poterli estrarre ai fini probatori per l'eventuale denuncia querela alle autorità competenti.
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

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.
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.
L'Università garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza.
In particolare:

1. 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;
2. solo il personale autorizzato può avere accesso alle immagini;
3. il personale autorizzato è tenuto al segreto professionale;
4. 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:

1. adottare le garanzie di cui all'art. 4 della legge del 20 maggio 1970, n. 300;
2. garantire l'osservanza dei principi di necessità, finalità e proporzionalità del trattamento dei dati;
3. 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;
4. 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 un contenzioso.

Resta ferma la necessità di effettuare una valutazione di impatto (DPIA), ai sensi dell'art.35, comma 3, lettera c) del Regolamento UE, ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.
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

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

Nell'ambito delle attività connesse al funzionamento degli organi collegiali il trattamento dei dati personali avviene in conformità del presente Regolamento e al solo fine della corretta gestione del processo deliberativo.

ARTICOLO 34 - DISPOSIZIONI FINALI

Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento UE e del D. Lgs. 196/2013 Codice per la protezione dei dati personali e ss.mm.ii., oltre a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dal Garante.
Costituiscono parte integrante e sostanziale del presente Regolamento gli allegati che ad esso si riferiscono in quanto connessi ad ambiti specifici dallo stesso disciplinati, compresi eventuali allegati modificati, aggiornati o integrati sulla base di specifiche normative. Di eventuali modifiche, integrazioni, aggiornamenti degli allegati al presente Regolamento si darà atto tramite annotazione Titulus sulla registrazione a protocollo del Decreto Rettorale di emanazione del presente Regolamento.

ARTICOLO 35 - TEMPORALE E PUBBLICITA'

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.
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.