SAPIENZA
UNIVERSITÀ DI ROMA

# REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

## SOMMARIO

## TITOLO I
## DISPOSIZIONI GENERALI

### Articolo 1 - Ambito di applicazione

1. Il presente Regolamento, adottato in attuazione del Regolamento Generale sulla Protezione dei Dati, Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016 (anche RGPD) e del Codice in materia di protezione dei dati personali, il d. lgs. n. 196/2003 come novellato dal d. lgs. n. 101/2018 (di seguito Codice *privacy*) e da successive modifiche, disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi all'interno di Sapienza Università di Roma (di seguito Università o Sapienza).
2. L'Università in qualità di Titolare del trattamento effettua i trattamenti dei dati personali con o senza ausilio di processi automatizzati e il presente Regolamento detta regole finalizzate ad assicurare la conformità dei trattamenti dei dati alla normativa citata.
3. I dati personali sono trattati per lo svolgimento dei propri fini istituzionali, nel rispetto dello Statuto, delle leggi e dei regolamenti vigenti e nel rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato, nonché del diritto alla protezione dei dati personali.
4. 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.
5. 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 e dagli altri atti adottati da Sapienza, in conformità alla normativa vigente.

### Articolo 2 – Definizioni

1. Ai fini del presente regolamento, nel rinviare per le ulteriori definizioni alla normativa vigente, nonché alla prassi europea e nazionale in materia di protezione dei dati personali, si intende per:
a) **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;
b) **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;
c) **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;
d) **dati genetici**: i dati personali relative alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
e) **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;
f) **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;
g) **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;
h) **responsabile esterno del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
i) **responsabile interno/designato:** i responsabili delle strutture ai quali sono attribuite funzioni organizzative o cariche istituzionali.
j) **autorizzati al trattamento/incaricati**: le persone fisiche formalmente autorizzate e istruite a trattare i dati personali sotto l'autorità diretta del Titolare e/o del Responsabile interno/Designato, per le finalità stabilite dal Titolare (artt. 4, 29, 32, 39 del regolamento UE);
k) **amministratore di sistema** (per brevità anche AdS): in mancanza di una definizione normativa, nel provvedimento del Garante *privacy* del 27 novembre 2008, l'AdS è la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
l) **interessato al trattamento**: la persona fisica alla quale si riferiscono i dati personali;
m) **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;
n) **terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile esterno del trattamento, il responsabile interno del trattamento e le persone

autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
o) **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;
p) **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;
q) **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;
r) **limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
19. **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;
s) **responsabile per la protezione dei dati (RPD o DPO)**: figura specializzata nel supporto al Titolare del trattamento prevista come obbligatoria negli enti pubblici;
t) **registro attività di trattamento**: elenco, in forma cartacea o digitale, delle attività di trattamento dei dati personali effettuate sotto la propria responsabilità dal Titolare e dal Responsabile esterno/Designato per la protezione secondo le rispettive competenze;
u) **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.
v) **violazione dei dati personali (o *data breach*)**: 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;
w) **autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro: per l'Italia il Garante per la protezione dei dati personali (per brevità anche Garante *privacy*);
x) **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.

## Articolo 3 - Principi generali

1. Il trattamento dei dati personali viene effettuato dall'Università in applicazione dei principi previsti dall'art. 5 e 25 del Regolamento UE 2016/679.
2. In particolare, i dati personali sono:
   a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (in conformità ai principi di liceità, correttezza e trasparenza);
   b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità (limitazione della finalità).
   Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
   c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (nel rispetto del principio di minimizzazione dei dati);
   d. esatti e, se necessario, aggiornati.
   A tal fine sono adottate le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati (esattezza);
   e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, a condizione dell'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE (limitazione della conservazione);
   f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale, compresa la protezione, mediante misure tecniche e organizzative adeguate (integrità e riservatezza).
3. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, l'Università adotta misure tecniche e organizzative adeguate in grado di comprovare il rispetto dei principi di cui al precedente comma (responsabilizzazione/*accountability*).
4. Tutti i soggetti che a vario titolo sono coinvolti nella attività di trattamento dei dati personali, devono garantire il rispetto dei principi in materia di protezione dei dati personali e la corretta applicazione del presente regolamento e, più in generale, delle disposizioni applicabili in tema di trattamento dei dati personali.
5. L'Università, adottando l'approccio dell'*accountability/*responsabilizzazione, considera la protezione dei dati personali sin dal momento della progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*).
6. Nel caso di trasferimento dei dati personali verso un Paese terzo o un'organizzazione internazionale trovano applicazione le specifiche condizioni previste dagli artt. 44 e ss. del RGPD al fine di garantire il livello di protezione delle persone fisiche previsto dalla normativa europea.

### Articolo 4 - Base giuridica

1. L'Università può trattare i dati personali quando occorre una delle altre condizioni previste dall'art. 6, par. 1 e dall'art. 9, par. 2 del RGPD.
2.1 L'Università è una pubblica amministrazione ai sensi dell'art. 1, c. 2 del d. lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche.
2.2 I trattamenti dei dati personali effettuati dall'Università per il perseguimento delle finalità istituzionali e dei compiti ad esse connesse non necessitano del consenso dell'interessato e trovano fondamento nella base giuridica prevista dall'art. 6, par. 1, lett. e) del RGPD.
2.3 Come previsto dall'art. 2-*ter* del d.lgs. 196/2003 e ss.mm.ii., la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di poteri pubblici è costituita da una norma di legge o di regolamento o da atti amministrativi generali.
2.4 In base al comma 1-*bis* dell'art. 2-*ter* del d.lgs. 196/2003 e ss.mm.ii., fermo restando ogni altro obbligo previsto dal RGPD e dal Codice *privacy*, il trattamento dei dati personali da parte di un'amministrazione pubblica è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad essa attribuiti.
3. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato (principio di necessità).

## TITOLO II
## ORGANIGRAMMA DELLA PROTEZIONE DATI

### Articolo 5 - Titolare del trattamento

1. Sapienza Università di Roma, nella persona della Rettrice o del Rettore *pro-tempore* quale legale rappresentante, è Titolare del trattamento dei dati personali (anche Titolare) trattati dallo stesso Ateneo.
2. Sapienza applica la normativa in materia di protezione dei dati personali e adotta misure tecniche e organizzative adeguate a garantire e poter dimostrare la conformità del trattamento al Regolamento UE 2016/679 e al Codice *privacy*, tenendo conto della natura, dell'ambito di applicazione, del contesto, della base giuridica e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, modulati secondo la diversa probabilità e gravità. Le dette misure sono riesaminate e aggiornate periodicamente.
3. Per rendere operative le misure di cui al comma 2, Sapienza adotta il *Piano di conformità privacy* (per brevità anche Piano *privacy*), finalizzato a fornire indicazioni e raccomandazioni riguardo alle operazioni di trattamento dei dati personali effettuate nell'ambito dell'Ateneo, correlato dal relativo *Addendum*, che riporta in un'apposita tabella le specifiche azioni da intraprendere nel periodo di riferimento. Il Piano *privacy* di durata triennale è riesaminato e aggiornato dal Titolare, per adeguare le azioni che l'Ateneo dovrà intraprendere.
4. Costituisce una misura di sicurezza per l'applicazione del RGPD nell'ambito di Sapienza, la distribuzione al suo interno dei ruoli *privacy* e delle responsabilità inerenti alle figure dell'organigramma della protezione dati.

## Articolo 6 - Contitolare

1. Nel caso in cui Sapienza determini le finalità e i mezzi di un trattamento congiuntamente ad un altro soggetto, sia pubblico che privato, quest'ultimo assume il ruolo di Contitolare del trattamento.
2. I Contitolari definiscono in uno specifico accordo interno, redatto in forma scritta, i rispettivi ruoli e responsabilità in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riguardo all'esercizio dei diritti dell'interessato, nonché alle rispettive funzioni di comunicazione delle informazioni richieste dall'informativa *privacy*.
3. Il contenuto essenziale dell'accordo interno di cui al comma 2 è messo a disposizione degli interessati, i quali possono esercitare i propri diritti nei confronti di ciascun Contitolare del trattamento.

## Articolo 7 – Responsabile esterno del trattamento

1. Il Responsabile esterno del trattamento è il soggetto esterno che, per mezzo di un contratto/convenzione o altro atto giuridico avente forma scritta, esegue i trattamenti dei dati personali per conto di Sapienza e ne risponde in solido in caso di inadempienze.
2. Il Responsabile esterno, nominato con atto giuridico conforme al diritto nazionale e all'art. 28 del RGPD, deve fornire idonee garanzie, soprattutto in relazione alle misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni del RGPD. Al responsabile esterno spettano, all'interno del proprio organismo, i compiti del Titolare (valutazione di impatto, registro dei trattamenti, eventuale nomina del proprio RPD, ecc.).
3. L'atto di nomina del Responsabile esterno del trattamento determina la natura, la durata e la finalità del trattamento o dei trattamenti assegnati, il tipo di dati trattati, le categorie di interessati, gli obblighi e i diritti del Titolare e del Responsabile.
4. Per specifiche attività di trattamento, il Responsabile esterno individuato non può nominare un altro Responsabile (sub-responsabile) se non con autorizzazione scritta del Titolare. Nei contratti con i sub-responsabili del trattamento devono essere riportati gli stessi obblighi contrattuali in materia di protezione dei dati personali previsti dal contratto che lo lega alla Sapienza.
5. Qualora un sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti della Sapienza l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.
6. Sapienza può a sua volta essere nominata Responsabile di uno o più trattamenti di dati personali quando li effettua, in base ad un contratto/convenzione o altro atto giuridico avente forma scritta, per conto di un altro Titolare. In questi casi è redatto anche il Registro delle attività dei trattamenti eseguiti per conto del Titolare, con le informazioni previste dall'art. 30 par. 2 del RGPD.

## Articolo 8 - Designati al trattamento

1. Il Titolare, nell'adempimento delle prescrizioni dettate dalla normativa comunitaria e nazionale in tema di protezione dei dati personali ed a garanzia della conforme gestione degli stessi, individua le seguenti figure di Responsabili di Struttura, sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono, quali Designati al trattamento: la Direttrice/il Direttore Generale, le Dirigenti e i Dirigenti delle Aree dell'Amministrazione Centrale, o i Capi Ufficio delle Aree, in loro mancanza, la/il Responsabile dell'Ufficio dell'Esperto Qualificato, le Direttrici e i Direttori del Centro di Medicina occupazionale, del Centro InfoSapienza, del Laboratorio Chimico per la Sicurezza, del Sistema Bibliotecario e del Polo museale, i Capi dei seguenti Uffici: Ufficio Speciale prevenzione, protezione e Alta Vigilanza, Ufficio Organi Collegiali e Ufficio Procedimenti Disciplinari, le Presidi e i Presidi di Facoltà e della Scuola di Ingegneria Aerospaziale, le Direttrici e i Direttori di Dipartimento e della Scuola Superiore di Studi Avanzati, le Direttrici e i Direttori dei Centri di ricerca, dei Centri di ricerca e servizi e dei Centri di servizi.
2. Nell'ambito organizzativo dell'Ateneo, la Rettrice o il Rettore, in qualità di legale rappresentante della Sapienza nomina, con apposito atto, il Designato del trattamento il quale è istruito ed agisce per conto del Titolare ed ha i seguenti compiti:
- vigilare, monitorare e garantire, all'interno della struttura cui è preposto, il rispetto delle norme vigenti e delle istruzioni del Titolare in materia di protezione dei dati personali, individuando le modalità più opportune per autorizzare, il personale afferente alla Struttura, al trattamento dei dati personali;
- collaborare, per la parte di propria competenza, nella mappatura dei trattamenti, nel censimento delle banche dati e dei trattamenti di dati esternalizzati e nella implementazione e aggiornamento del registro dei trattamenti;
- predisporre ed aggiornare l'informativa *privacy* e la relativa modulistica;
- impartire idonee istruzioni in materia di informativa *privacy* e di misure di sicurezza al personale autorizzato al trattamento;
- vigilare sul rispetto delle misure di sicurezza finalizzate ad evitare i rischi, anche accidentali, di distruzione o perdita di dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta;
- conservare, per quanto di competenza, e rendere disponibile su richiesta del Titolare o del RPD copia della seguente documentazione: nomine di incaricati, accordi stipulati con i Responsabili esterni, registro dei trattamenti dei responsabili esterni in caso di nomina, report delle Valutazioni di impatto *privacy* (DPIA), valutazioni dei trattamenti basati sul legittimo interesse, comunicazioni delle violazioni di dati personali (*data breach*), informative agli interessati relative ai trattamenti effettuati.

## Articolo 9 - Responsabile scientifico

1. Il personale docente (professoresse e professori, ricercatrici e ricercatori) della Sapienza, che opera in qualità di Responsabile scientifico in progetti e/o ricerche in ambito universitario, in quello di enti ed istituti di ricerca e di società scientifiche, quando tratta dati personali a fini statistici o scientifici è tenuto a garantire i necessari standard di sicurezza e protezione dei dati, secondo le prescrizioni del presente Regolamento e degli altri atti adottati in materia di protezione dei dati

personali.
2. Il personale di cui al comma 1, oltre ad attenersi al rispetto delle disposizioni normative comunitarie e internazionali relative al trattamento dei dati personali a fini statistici e scientifici, deve operare in conformità alle Prescrizioni e Regole deontologiche adottate e approvate dal Garante per la protezione dei dati personali e condividere le buone pratiche adottate o adottabili nell'ambito delle ricerca storica, scientifica e statistica al fine di garantire una maggiore protezione dei dati personali e aderenza al RGPD.
3. Nell'ambito del trattamento dei dati personali per finalità di ricerca, spetta al Responsabile scientifico: garantire il rispetto del principio di minimizzazione, non raccogliendo dati non necessari per il perseguimento delle finalità di ricerca; informare adeguatamente gli interessati e predisporre adeguate misure tecniche e organizzative per garantire la protezione dei dati personali, a seguito di un'analisi dei rischi.
4. Il responsabile scientifico, nell'ambito di una ricerca con trattamento di dati personali informa il Designato della struttura di afferenza.
5. Relativamente al trattamento dei dati personali, se necessario, il responsabile scientifico chiede il parere, la valutazione o la verifica al Comitato Etico della Ricerca Transdisciplinare di Sapienza nelle tematiche di ricerca di sua competenza.

## Articolo 10 - Incaricati del trattamento

1. L'Incaricato del trattamento dei dati è il soggetto, individuato dal Titolare o dai Designati, che, in forza del ruolo ricoperto all'interno della Sapienza, viene autorizzato a compiere operazioni di trattamento sui dati personali.
2. Gli Incaricati sono autorizzati al trattamento dei dati mediante formale nomina individuale o collettiva, da parte del Titolare o dei Designati, ed operano sotto la loro vigilanza.
3. La designazione dell'Incaricato avviene con atto scritto, nel quale sono fornite le istruzioni necessarie a garantire il corretto trattamento dei dati personali gestiti, secondo le finalità perseguite dalla Sapienza, e nel rispetto dei principi generali in materia di protezione dei dati personali.
4. In attesa/assenza di formale designazione degli incaricati, coloro che trattano dati personali per l'afferenza alla Struttura universitaria di appartenenza in virtù di vincolo contrattuale con la Sapienza, sono istruiti e ritenuti autorizzati al trattamento per la provata appartenenza all'unità organizzativa di riferimento, quindi tenuti al rispetto delle prescrizioni del presente Regolamento.
5. L'Incaricato si impegna ad effettuare i trattamenti dei dati personali in osservanza delle misure di sicurezza previste dalla Sapienza, al fine di evitare rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito dei dati personali.
6. In particolare, l'Incaricato è tenuto a:
- mantenere il segreto e la riservatezza sull'attività prestata, sulle informazioni e su tutti i dati di cui sia venuto a conoscenza durante tale attività;
- 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 Incaricato;
- seguire i corsi d'informazione e formazione in materia di protezione dei dati personali organizzati dalla Sapienza;

- osservare le misure tecniche e organizzative indicate dall'Ateneo, anche per il tramite dei Designati, al fine di garantire la sicurezza del trattamento dei dati personali, anche da remoto;
- curare, in occasione delle operazioni di trattamento di dati personali, che tali dati non siano soggetti a rischi di distruzione o perdita; inoltre, si assicura che le informazioni non siano accessibili a persone non autorizzate e comunque che non siano svolte operazioni di trattamento non consentite;
- segnalare con tempestività al proprio Responsabile di Struttura/Designato eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, la procedura di comunicazione delle violazioni di dati al RPD.

7. Il Titolare o i Designati possono autorizzare quale Incaricato del trattamento un soggetto terzo che debba svolgere operazioni di trattamento di dati personali, ad esclusione dei dati sensibili, per un periodo limitato di tempo, secondo le indicazioni di cui al comma 3.
8. Nel caso in cui l'Incaricato nutra dei dubbi sulle operazioni da intraprendere o sulla legittimità del trattamento, deve darne tempestiva comunicazione al Designato e, in caso di irreperibilità, al RPD.

## Articolo 11 - Amministratori di sistema

1. Gli Amministratori di sistema sono i soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati e delle sue componenti, utilizzati in relazione ai trattamenti dei dati personali effettuati all'interno della Sapienza. Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e per la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali.
2. Ai fini del presente Regolamento, sono considerati Amministratori di sistema le figure professionali che operano in Sapienza per l'amministrazione di basi di dati, di reti, di apparati di sicurezza e di sistemi software complessi.
3. Il Titolare o il Designato individua gli Amministratori di sistema con formale atto di designazione individuale, nel quale sono definiti in maniera analitica i compiti e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, secondo le specifiche direttive fornite in merito dal Garante per la protezione dei dati personali.
4. Nel caso di notificazioni di violazioni di sicurezza dei dati, l'Amministratore di sistema notifica al Designato e al RPD eventuali anomalie riscontrate, malfunzionamenti o rischi di sicurezza.
5. L'Amministratore di sistema supporta i Designati e gli Incaricati per gli aspetti di tipo tecnico-informatico nello svolgimento delle consuete attività operative istituzionali.
6. Il Titolare adotta dei sistemi di controllo che consentano la registrazione degli accessi effettuati dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e sono essere conservate per un congruo periodo, non inferiore a sei mesi.
7. L'operato degli Amministratori di sistema è oggetto di verifica da parte del Centro InfoSapienza.

## Articolo 12 - Responsabile della protezione dei dati (RPD)

1. Il Responsabile della Protezione dei Dati (RPD) è una figura specializzata di 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.
2. Il RPD è individuato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti.
3. Il RPD può essere un soggetto interno (dipendente dell'Università) o esterno, nel qual caso assolve i suoi compiti in base a un contratto di servizi; nel caso di soggetti interni, è nominato con decreto della/del Rettrice/Rettore.
4. I principali compiti che il RPD è tenuto a svolgere sono i seguenti:

- informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa comunitaria e nazionale relativa alla protezione dei dati;
- sorvegliare l'osservanza del presente Regolamento e degli altri atti in materia di protezione dei dati personali adottati in Sapienza, del Regolamento Generale sulla Protezione dei Dati - RGPD 2016/679, del Codice *privacy* e delle altre disposizioni derivanti dalla normativa comunitaria e nazionale, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con il Garante per la protezione dei dati personali;
- fungere da punto di contatto per il Garante *privacy* per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- collaborare nella redazione e aggiornamento dei Registri delle attività di trattamento;
- svolgere ogni ulteriore compito attribuito dal Titolare.

5. Nell'eseguire i propri compiti, il RPD tiene in debito conto i rischi inerenti al trattamento, considerata la natura, l'ambito di applicazione, il contesto e le finalità del medesimo.
6. Al RPD sono garantiti il supporto, le risorse e tempi di lavoro adeguati allo svolgimento della sua funzione, per la quale può avvalersi di specifici gruppi di lavoro in materia di adeguamento alla normativa di settore. È garantita, altresì, una formazione permanente specialistica che gli consenta un costante aggiornamento sugli sviluppi nel settore della protezione dei dati.
7. Il RPD ha ampio accesso alle informazioni necessarie per svolgere i propri compiti ed è interpellato per ogni problematica inerente alla protezione dei dati e per le attività che implicano un trattamento dei dati fin dalla progettazione e per impostazione predefinita.
8. Il Titolare garantisce che il RPD eserciti le proprie funzioni in autonomia e indipendenza; in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o conflitto di interesse con il suo ruolo e le sue funzioni istituzionali.

9. Il RPD non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati e non può essere rimosso o penalizzato in ragione degli adempimenti svolti nell'esercizio delle sue funzioni.
10. Il RPD invia alla/al Rettrice/Rettore e alla/al Direttrice/Direttore Generale una relazione annuale sullo stato di implementazione dei processi volti a garantire il rispetto della normativa in materia di protezione dei dati personali all'interno della Sapienza, sull'attività compiuta nel periodo di riferimento e sullo stato di attuazione delle azioni previste dall'*Addendum* al Piano di conformità *privacy*, nonché sulle linee generali di intervento per il periodo successivo.
11. Il nominativo e i dati di contatto del RPD sono comunicati al Garante *privacy* e sono pubblicati sul sito istituzionale della Sapienza, alla pagina dedicata al Settore *privacy*, di cui al successivo articolo 14. I dati di contatto del RPD sono~~,~~ inseriti nelle informative *privacy.*

## TITOLO III
## TIPOLOGIE DI TRATTAMENTO DEI DATI

### Articolo 13 - Trattamento dei dati personali

1. Sapienza effettua, con misure adeguate e tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, il trattamento di dati personali per lo svolgimento delle proprie finalità istituzionali di interesse pubblico, come individuate da disposizioni normative, statutarie e nel rispetto del RGPD, del Codice in materia di protezione dei dati personali, nonché delle Linee guida e dei provvedimenti emanati dal Garante *privacy*.
2. I dati personali devono essere trattati secondo le finalità e con le modalità descritte al precedente articolo 3, e i trattamenti possono riguardare, a titolo esemplificativo e non esaustivo:

- la gestione del rapporto di lavoro del personale docente, del personale dirigente e tecnico–amministrativo, dei collaboratori e delle collaboratrici esterni/e, nonché dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato;
- l'attività didattica e la gestione della carriera delle studentesse e degli studenti, ivi compresi laureate/i, dottorande/i di ricerca, specializzande/i e tirocinanti;
- l'attività di ricerca, compresa la ricerca in ambito medico, le attività didattiche e assistenziali connesse alla ricerca, le attività assistenziali effettuate nell'ambito delle strutture ospedaliere e sanitarie convenzionate;
- le attività gestionali e contrattuali, conto terzi e/o connessi ad attività trasversali, ivi compreso il trasferimento tecnologico.

### Articolo 14 - Trattamento di categorie particolari di dati

1. Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché quello 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 (cd. Categorie particolari di dati) è ammesso solo in

presenza di una delle condizioni di seguito elencate:

a) l'interessato ha prestato il consenso esplicito per una o più finalità specifiche;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti della Sapienza o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o nazionale o da un contratto collettivo, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale della persona interessata o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestatamente pubblici dall'interessato;
e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
f) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o nazionale o conformemente al contratto con un professionista della sanità e i dati sono trattati da o sotto la responsabilità di un professionista soggetto a segreto professionale;
g) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, in conformità alle disposizioni dell'art. 89 del Regolamento UE;
h) il trattamento è necessario per motivi di interesse pubblico rilevante, se previsto dal diritto dell'Unione o dall'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili, e il motivo di interesse pubblico rilevante, nonché che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Ai fini delle disposizioni di cui al precedente comma 1, lettera h), sono considerati di rilevante interesse pubblico i trattamenti eseguiti nelle materie previste dall'art. 2-*sexies* del Codice *privacy*:

3. I dati genetici, biometrici e relativi alla salute non possono essere diffusi e possono essere trattati solo in presenza di una delle condizioni di cui al comma 1 e in conformità alle misure di protezione disposte dal Garante *privacy*.

## Articolo 15 - Trattamento di dati relativi a condanne penali e reati

1. Il trattamento di dati personali relativi a condanne penali e a reati, oppure a connesse misure di sicurezza (**dati c.d. "giudiziari")** è ammesso solo se autorizzato dal diritto dell'Unione o dall'ordinamento nazionale che preveda garanzie appropriate per i diritti e le libertà degli interessati.

2. Il trattamento dei dati di cui al comma 1 è ammesso, in particolare, nei seguenti casi, previsti dall'art. 2-*octies* del Codice *privacy*:

a) 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 e 88 del RGPD;
b) adempimento di obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione di controversie civili e commerciali;
c) verifica o accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
d) 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;
e) accertamento, esercizio o difesa di un diritto in sede giudiziaria;
f) esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
g) 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;
h) 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;
i) 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 16 - Trattamenti principali inerenti alle studentesse e agli studenti

1. Sapienza effettua il trattamento dei dati personali delle studentesse e degli studenti, intesi nella loro accezione più ampia (ovvero coloro che frequentano i corsi di studio e/o fruiscono dell'offerta formativa della Sapienza, ivi compresi, a titolo esemplificativo e non esaustivo, dottorande/i di ricerca, specializzande/i, studentesse e studenti iscritti presso altre Università, anche straniere, che frequentano l'Ateneo a qualunque titolo per fini didattici e/o di ricerca, laureate/i, tirocinanti), per lo svolgimento delle procedure di ammissione e di immatricolazione ai corsi di laurea, post-laurea e tirocini, nonché di tutte le attività relative alla gestione della carriera dello studente.
2. Sapienza garantisce il rispetto delle vigenti disposizioni in materia di pubblicazione dell'esito degli esami tramite canali telematici dedicati e/o affissione presso le sedi delle Strutture didattiche dell'Ateneo e di rilascio di diplomi e certificati. Nelle pubblicazioni si utilizza ove possibile il numero di matricola e in ogni caso, i dati pubblicati per via telematica o affissione non devono fornire, anche indirettamente, informazioni sullo stato di salute e sulle situazioni di particolare disagio personale, anche economico, degli studenti.
3. Nello svolgimento delle attività didattiche e degli esami, anche a distanza, Sapienza effettua il trattamento dei dati personali di docenti, di loro eventuali collaboratori e collaboratrici, nonché delle studentesse e degli studenti, con o senza strumenti informatizzati, nei limiti di quanto strettamente necessario, pertinente e non eccedente rispetto alle finalità di cui ai commi precedenti del presente articolo.

## Articolo 17 - Trattamenti principali inerenti a dipendenti e collaboratori

1. Sapienza effettua il trattamento dei dati personali del personale docente, del personale dirigente e tecnico-amministrativo e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato, adottando le opportune garanzie tese ad assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi applicabili.
2. Il trattamento, da parte della Sapienza, dei dati personali relativi al personale dipendente non richiede il loro consenso esplicito, nel caso sia necessario per:

- motivi di interesse pubblico rilevante, come definiti dal Codice in materia di protezione dei dati personali;
- assolvere gli obblighi ed esercitare i diritti specifici del Titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- accertare, esercitare o difendere un diritto in sede giudiziaria;
- finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità all'art. 89 del RGPD.

4. Nel caso di prestazione lavorativa effettuata in modalità da remoto, questa viene, di regola, effettuata attraverso strumenti e/o servizi informatici messi a disposizione dal Titolare.

## Articolo 18 - Trattamenti trasversali

1. Quando il trattamento dei dati è effettuato per più finalità e richiede lo svolgimento di plurime attività, assume il carattere della trasversalità; tale caratteristica deve essere correttamente recepita nelle relative Informative, con la specificazione della natura dei dati personali trattati, delle varie finalità da perseguire e con la puntuale descrizione del trattamento.
2. Sapienza effettua il trattamento trasversale dei dati e/o i trattamenti connessi ad attività trasversali, nei seguenti casi, elencati in via esemplificativa ma non esaustiva:

a) Trattamento dei dati nell'ambito della gestione degli spazi: il dato è trattato al fine di permettere l'utilizzo degli spazi dell'Ateneo, per attività quali:
   1) assegnazione degli spazi alle strutture, allocazione delle persone negli spazi;
   2) controllo accessi ai varchi da parte di: dipendenti, collaboratori e studenti;
   3) la gestione centralizzata e coordinata delle aule e degli spazi per la didattica;
   4) la gestione delle procedure amministrative per richieste di spazi per eventi istituzionali;
   5) la gestione delle procedure amministrative per richieste di spazi da parte di soggetti terzi.

b) Trattamento dei dati personali per la gestione delle postazioni
   Il dato è trattato per garantire il corretto funzionamento di postazioni di lavoro fisse/mobili assegnate agli utenti, la sicurezza delle stesse e per fornire il necessario supporto nell'utilizzo.

c) Trattamento per attività di gestione degli organi e delle cariche istituzionali, che comprende il:

c1) *Trattamento finalizzato alla gestione degli elenchi per l'elettorato attivo e passivo*
Il dato è trattato, nell'ambito del rinnovo degli organi istituzionali, per la gestione degli elenchi dell'elettorato attivo e passivo, per le sostituzioni dei componenti e per verificare i requisiti di eleggibilità.
c2) *Trattamento finalizzato alla nomina degli eletti e delle cariche accademiche*
Il dato è trattato ai fini della gestione della nomina degli eletti e dalle cariche accademiche, nonché per la verifica della presenza di eventuali cause di incompatibilità con la carica da assumere.
c3) *Trattamento finalizzato alla pubblicizzazione di atti ai fini di trasparenza*
Il dato è trattato per finalità di trasparenza come da normativa vigente sul sito istituzionale per la parte di "Amministrazione Trasparente".

d) Trattamento per la gestione degli infortuni
Il trattamento viene effettuato in relazione agli infortuni occorsi al personale docente, tecnico amministrativo, agli studenti ed ai soggetti terzi in visita.

e) Trattamento in ambito bibliotecario
Il dato è trattato al fine di consentire al personale docente, tecnico amministrativo, popolazione studentesca e ai cittadini, di accedere ai servizi centralizzati offerti dal sistema bibliotecario e ai locali e servizi offerti dalle singole Biblioteche di Ateneo (consultazione e prestito patrimonio bibliografico e documentale su supporto cartaceo e elettronico, prestito interbibliotecario e *document delivery*, *reference*, ecc.) e per informazione sulle attività e servizi offerti.

f) Trattamento di dati nell'ambito dei servizi di protocollo e conservazione documentale, che comprende il:
f1) *trattamento finalizzato alla gestione del protocollo in entrata/uscita*
I dati sono trattati nell'ambito della gestione del protocollo informatico nelle fasi di entrata/uscita al fine di fornire data e ora certa agli atti acquisiti o trasmessi da una Pubblica Amministrazione.
f2) *trattamento finalizzato alla conservazione documentale*
I dati sono trattati nell'ambito della gestione delle attività di conservazione documentale ai sensi della normativa vigente.

g) Trattamento finalizzato all'acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso, che comprende il:
g1) *trattamento finalizzato all'acquisizione di beni e servizi*
Il dato è trattato per consentire la verifica di posizioni giudiziarie, fiscali e di condotta di fornitori ed operatori economici che sono in rapporto con l'Ateneo.
g2) *trattamento finalizzato alle verifiche sull'espletamento di lavori, in cantiere o presso installazioni in Sapienza*
Il dato è trattato per la valutazione amministrativa ed economica di terzi, fornitori dell'Ateneo per l'espletamento di lavori in appalto, verifiche sui cantieri o presso installazioni in Ateneo.
g3) *trattamento finalizzato alla gestione del contenzioso e del recupero crediti*
Il dato è trattato per:
- la gestione dei contenziosi instaurati avanti le diverse autorità giudiziarie in cui sia coinvolta l'Università;

- l'attività di recupero dei crediti dell'Università nei confronti di personale docente/ricercatore e tecnico-amministrativo, degli studenti e di soggetti terzi inadempienti.

h) Trattamento di dati nell'ambito dei servizi di posta elettronica e strumenti di collaborazione, che comprende il:

h1) *trattamento finalizzato all'accesso agli strumenti di collaborazione*

In ambito di collaborazione, Sapienza potrebbe fornire strumenti informatici (es: web conference, spazi virtuali di collaborazione, ecc..) tramite i quali possono essere trattati dati personali funzionali:

- all'erogazione del servizio stesso;
- a connesse attività di risoluzione dei guasti (*troubleshooting*);
- alla valutazione dell'uso del servizio e della qualità (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti)
- a garantire la sicurezza informativa dei dati trattati mediante tali strumenti di collaborazione.

h2) *trattamento finalizzato all'erogazione di servizi di posta elettronica*

Allo scopo di favorire la comunicazione istituzionale tramite i servizi di posta elettronica, Sapienza potrebbe trattare dati personali funzionali a:

- l'erogazione del servizio stesso;
- lo svolgimento attività connesse alla risoluzione dei guasti (*troubleshooting*);
- la valutazione dell'uso del servizio e della qualità del servizio (es: mediante rilevazioni statistiche basate sull'uso di tali strumenti);
- garantire la sicurezza informativa dei dati trattati (tramite ad esempio la gestione di incidenti di sicurezza e tramite azioni preventive sulla diffusione di messaggi contenenti malware).

## Articolo 19 - Trattamento dei dati nelle sedute degli organi collegiali

1. Nel corso delle sedute degli Organi Collegiali della Sapienza (Senato Accademico e Consiglio di Amministrazione), il trattamento dei dati correlati agli argomenti in trattazione, comunicati dalle Strutture dell'Ateneo in qualità di promotrici e referenti dei punti all'ordine del giorno, avviene in conformità alle prescrizioni del presente Regolamento.
2. Le finalità del trattamento di cui al comma 1 sono connesse all'espletamento delle attività istruttorie da parte dei componenti degli Organi suddetti, per l'adozione delle delibere di competenza degli stessi.

## Articolo 20 - Trattamento dei dati personali a fini di archiviazione, di ricerca scientifica o storica e a fini statistici

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato da chiunque operi nell'ambito delle Strutture della Sapienza garantendo il rispetto del principio della minimizzazione dei dati.
2. 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.
3. 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 RGPD.
4. 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.
5. 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.
6. 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 *privacy*.
7. Il trattamento di dati personali ai fini statistici o di ricerca scientifica da parte di chiunque operi all'interno di Uffici e Strutture della Sapienza o per conto della Sapienza stessa, deve avvenire nel rispetto dei seguenti principi:

a) i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né trattati per altri scopi;
b) all'interessato deve essere fornita puntuale informazione relativamente alle finalità statistiche o di ricerca scientifica del trattamento, 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.

## TITOLO IV
## PROTEZIONE E SICUREZZA DEI DATI

### Articolo 21 - Registri delle attività di trattamento

1. L'Università, in qualità di Titolare del trattamento, ha un Registro delle attività di trattamento svolte sotto la propria responsabilità.
2. Il Registro contiene le seguenti informazioni:
a) la struttura competente in ordine al trattamento;
b) ove esistenti, i nominativi e i dati di contatto del/i Contitolare/i e del/i Responsabile/i del trattamento;
c) le finalità del trattamento;
d) una descrizione delle categorie di interessati e delle categorie di dati personali;
e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
f) l'eventuale trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, con l'indicazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
h) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
3. Il Titolare, anche tramite i Designati, tiene aggiornato detto Registro, nel caso di inizio o cessazione di un trattamento e nel caso si renda necessaria la modifica

dei trattamenti dei dati già presenti nel Registro di Ateneo.
4. L'Università tiene altresì un Registro di tutte le categorie di trattamenti svolti in qualità di Responsabile per conto di altri Titolari di trattamento, contenente:
a) la struttura competente in ordine al trattamento;
b) il nominativo e i dati di contatto del Titolare per conto del quale l'Università agisce e del Responsabile della protezione dei dati;
c) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
d) l'eventuale trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, con l'indicazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
e) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
5. I Registri, tenuti in forma scritta, anche in formato elettronico, sono messi a disposizione del Garante *privacy* o dei danti causa dietro motivata richiesta.

## Articolo 22 - Formazione e sensibilizzazione del personale

1. Al fine della corretta e puntuale applicazione della disciplina in materia di protezione dei dati personali e della sicurezza informatica, l'Università sostiene e promuove, con il coinvolgimento degli organi istituzionali dell'Ateneo competenti per materia, strumenti di sensibilizzazione e attività formative (in aula, webinar o linee guida) finalizzati a consolidare la consapevolezza del valore della protezione dei dati personali e indirizzate al personale dell'Ateneo e a coloro che intrattengono rapporti con l'Ateneo.

## Articolo 23 - Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie e considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università, prima di procedere al trattamento, effettua, consultandosi con il RPD, una valutazione dell'impatto sulla protezione dei dati personali. Può essere condotta una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Fatte salve le tipologie di trattamento individuate dal Garante, la valutazione d'impatto viene effettuata dall'Università nei seguenti casi:

a) 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 significativamente analogo su dette persone;
b) trattamento su larga scala di categorie particolari di dati personali di cui al precedente art. 17 o di dati relativi a condanne penali e a reati;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
d) trattamento di dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

3. La valutazione di impatto contiene i seguenti elementi: a) una descrizione sistematica del trattamento e delle sue finalità; b) una valutazione in ordine alla necessità e alla proporzionalità del trattamento in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati; d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i

meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte.
4. Se necessario, l'Università procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto, quando insorgono variazioni del rischio rappresentato dalle attività di trattamento.
5. I Designati comunicano al Titolare tutti i nuovi trattamenti che intendono effettuare, per consentire allo stesso di effettuare, ove necessario, la valutazione di impatto.

## Articolo 24 - Consultazione preventiva

1. Ai sensi dell'art. 36 del RGPD, qualora la valutazione d'impatto sulla protezione dei dati indica che il trattamento presenta un rischio elevato, in assenza di possibili misure adottate dal Titolare del trattamento per attenuare il rischio, l'Università, per il tramite del RPD, prima di procedere al trattamento, consulta il Garante *privacy*.
2. In sede di consultazione, l'Università comunica al Garante *privacy*:
   a) le rispettive responsabilità dell'Università in qualità di Titolare, nonché di eventuali Contitolari e Responsabili del trattamento;
   b) le finalità e i mezzi del trattamento;
   c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
   d) i dati di contatto del RPD;
   e) la valutazione d'impatto sulla protezione dei dati;
   f) ogni altra informazione richiesta dal Garante *privacy*.

## Articolo 25 - Misure tecniche e organizzative

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, Sapienza in qualità di Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, misure che comprendono tra le altre la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'Università adotta un approccio che tiene conto della protezione dei dati personali oggetto di trattamento sin dal momento della progettazione (*by design*) e per impostazione predefinita (*by default*) anche nella scelta e nella configurazione dei sistemi informativi e delle procedure operative.
4. Il Titolare definisce le misure tecniche e organizzative, anche con specifiche *policy*/linee guida di cui verrà data ampia diffusione all'interno dell'Ateneo.
5. I soggetti autorizzati sono istruiti e formati nell'osservare le misure tecniche e

organizzative adeguate a limitare i rischi di distruzione o perdita, anche accidentale, e di accesso non autorizzato ai dati personali.
6. Ulteriori misure di sicurezza rispetto a quelle individuate dal Titolare, potranno essere implementate dai singoli soggetti Designati qualora risultino necessarie in relazione a specifiche esigenze della struttura gestita, tenuto conto del livello di esposizione al rischio individuato per peculiari attività di trattamento.
7. I soggetti Designati si coordinano con il Titolare nell'esecuzione dell'analisi dei rischi e dell'eventuale valutazione di impatto, adottando metodologie riconosciute a livello nazionale e internazionale.
8. Il Titolare monitora, anche per il tramite dei soggetti Designati, l'applicazione delle misure di sicurezza tecniche e organizzative all'interno dell'Università e presso i soggetti Responsabili del trattamento, adottando se del caso i necessari provvedimenti.

## Articolo 26 - *Privacy by design* nella progettazione degli impianti di elaborazione dell'Ateneo

1. Chiunque progetti o sviluppi impianti di elaborazione o suoi componenti hardware e software deve assicurare la rispondenza della soluzione alla normativa sul trattamento di dati personali sin dalla fase di progettazione e sviluppo dell'impianto, ivi compresi i profili relativi alla sicurezza.

## Articolo 27 - Violazione dei dati personali (*data breach*) e sanzioni

1. In caso di violazione dei dati personali, l'Università, con comunicazione del RPD, notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica al Garante non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. La notifica deve contenere i seguenti elementi:
   a) natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti;
   b) nome e dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
   c) probabili conseguenze della violazione dei dati personali;
   d) misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
3. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
4. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università comunica la violazione all'interessato senza ingiustificato ritardo.
5. Non è richiesta la comunicazione all'interessato se ricorre una delle seguenti condizioni:
   a) l'Università ha messo in atto le adeguate misure, tecniche e organizzative,

di protezione (in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, come la cifratura) e tali misure erano state applicate ai dati personali oggetto della violazione;
b) l'Università ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) la comunicazione richiederebbe sforzi sproporzionati, nel qual caso si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

6. Nel caso in cui l'Università non abbia comunicato all'interessato la violazione dei dati personali, il Garante, dopo aver valutato la probabilità che la violazione presenti un rischio elevato, può richiedere che vi si provveda o può decidere che una delle condizioni di cui al comma 5 risulti soddisfatta.
7. L'Università documenta qualsiasi violazione dei dati personali, le relative circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio.
8. Il Settore Sicurezza informatica supporta il Titolare coordinandosi con il RPD nella gestione del *data breach*.
9. Il personale della Sapienza è tenuto a conformarsi alle ulteriori regole e istruzioni che sono adottate dall'Ateneo, soprattutto per quanto riguarda la comunicazione delle informazioni rilevanti e la cooperazione con gli Uffici competenti nella gestione del *data breach*.
10. Il Designato assicura, senza ingiustificato ritardo, l'invio all'indirizzo e-mail responsabileprotezionedati@uniroma1.it di tutte le informazioni utili alla gestione del *data breach*.

## TITOLO V
## DIRITTI DEGLI INTERESSATI

### Articolo 28 – I diritti dell'interessato

1. L'Università garantisce il rispetto dei diritti degli interessati di cui agli artt. da 12 a 22 del Regolamento UE 2016/679.

In particolare, l'interessato può:

a) ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
b) ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento;
c) esercitare il diritto alla limitazione del trattamento non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more del riscontro da parte del titolare di una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, o dell'accertamento dei diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante;
d) esercitare il diritto di opposizione alla profilazione;
e) esercitare il diritto alla portabilità dei dati solo qualora il trattamento si basi sul consenso ai sensi dell'art. 6. par. 1, lettera a), o dell'art. 9, par. 2, lettera a) del Regolamento UE o su un contratto ai sensi dell'art. 6, par. 1, lettera b) del

Regolamento UE e sia effettuato con mezzi automatizzati. Tale diritto non si applica al trattamento necessario per l'esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Università;
f) esercitare il diritto all'oblio chiedendo la cancellazione dei propri dati personali nel caso questi siano stati resi pubblici on-line. Tale diritto può essere esercitato ove ricorra una delle seguenti fattispecie:
I. i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
II. l'interessato revoca il consenso su cui si basa il trattamento;
III. l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
IV. i dati personali sono trattati illecitamente;
V. per l'adempimento di un obbligo legale;
VI. i dati riguardino minori.

## Articolo 29 - Esercizio dei diritti dell'interessato (*Vademecum*)

1. L'interessato può far valere, nei confronti dell'Ateneo, i propri diritti riconosciuti dal Regolamento UE 2016/679, compilando l'apposito modulo, allegato al *Vademecum* per l'esercizio dei diritti, pubblicato nella pagina web del Settore *Privacy* dell'Area Affari legali.
L'istanza, con allegata copia del documento di riconoscimento in corso di validità, può essere inoltrata al Titolare, anche tramite il Responsabile della protezione dei dati d'Ateneo (RPD), utilizzando qualsiasi canale (ad es. tramite e-mail, PEC, raccomandata postale con ricevuta di ritorno, ecc.); laddove l'interessato presenti la richiesta tramite strumenti elettronici, il Titolare o il RPD dovrà fornire le informazioni utilizzando a sua volta mezzi elettronici, salvo diversa indicazione dell'interessato.
2. L'istanza può essere presentata anche da parte di un delegato, fornendo copia della delega e del documento di riconoscimento del delegato e delegante. Le istanze pervenute direttamente al Titolare sono comunicate per conoscenza al RPD.
3. Il riscontro alla richiesta viene fornito senza ingiustificato ritardo, entro 30 giorni dalla data di acquisizione della richiesta, oppure, entro 60 giorni, nei casi di particolare e comprovata difficoltà. Le informazioni sono fornite all'interessato in forma scritta e, solo qualora quest'ultimo lo richieda, possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
4. L'Università agevola l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa. Nel *Vademecum* pubblicato nella pagina web del Settore *Privacy* dell'Area Affari legali, cui si rinvia, è esplicato il procedimento relativo alle richieste di esercizio dei diritti.

## Articolo 30 - Informazioni agli interessati

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

linguaggio chiaro e semplice.
2. L'informativa deve contenere:
- i dati di contatto dell'Università;
- i dati di contatto del Responsabile della Protezione dei Dati personali;
- le finalità del trattamento;
- la base giuridica del trattamento ai sensi dell'art. 4;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventuale volontà dell'Università di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di un fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai resi disponibili;
- il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;
- i diritti che l'interessato può esercitare, quali: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione, il diritto alla portabilità dei dati, la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, il diritto di proporre reclamo al Garante per la protezione dei dati personali;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.

3. Nel caso in cui i dati personali debbano essere trattati per una finalità diversa da quella per cui sono stati raccolti, l'Università fornisce all'interessato informazioni in merito alla diversa finalità prima di tale ulteriore trattamento.
4. Nel caso in cui i dati non siano raccolti presso l'interessato, l'Università si riserva la possibilità di non fornire l'informativa nel caso in cui l'interessato già disponga delle informazioni oppure comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.
5. L'informativa può non essere fornita nel caso in cui si prefiguri il rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.
6. Le informative di competenza delle strutture sono aggiornate dai Designati.
7. La modulistica, sia cartacea che digitale, che prevede la raccolta di dati riferiti a una persona fisica deve contenere almeno le seguenti informazioni:
- la finalità per cui i dati sono raccolti e per la quale saranno usati;
- l'indicazione di chi tratterà i dati all'interno dell'Università e se essi saranno resi disponibili a terzi;
- l'espressione del consenso ove questo fosse una condizione di liceità del trattamento.
8. Il personale e chiunque operi sotto l'autorità dell'Università può trattare i dati personali solo per le specifiche finalità indicate nell'informativa fornita all'interessato al momento del conferimento dei dati o per ogni altra finalità prevista dalla legge. I dati personali non possono essere usati per finalità diverse da quelle per le quali sono stati raccolti. Se si rendesse necessario modificare le finalità del trattamento, l'interessato dovrà essere informato della nuova finalità

prima dell'inizio di qualunque trattamento.

## TITOLO VI
## COMUNICAZIONE E DIFFUSIONE DEI DATI

### Articolo 31 – Circolazione dei dati all'interno dell'Ateneo

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

### Articolo 32 - Comunicazione e diffusione dei dati a soggetti terzi

1. La comunicazione e la diffusione dei dati personali, esclusi i dati relativi a origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati, sono permesse quando siano previste da norme di legge o di regolamento nei casi previsti dalla legge, o dal diritto dell'Unione europea;
2. La comunicazione di dati fra titolari che effettuano trattamenti di dati personali, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa per i fini istituzionali ove sia prevista da norma di legge o regolamento o da atti amministrativi generali.
3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità è disciplinato dall'art. 2-*ter* del Codice *privacy*.
4.1 Le richieste da parte di soggetti privati ed enti pubblici economici volte ad ottenere la comunicazione di dati, devono essere formulate per iscritto e motivate e devono contenere:
- il nome, la denominazione o la ragione sociale del richiedente;
- l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.

4.2 L'Università, nella figura del Titolare o Designato, valuta, sulla base di quanto disposto dalle norme vigenti in materia di protezione dei dati personali e di quanto previsto dal presente Regolamento, le eventuali richieste di comunicazione di dati personali a soggetti privati e decide in ordine all'opportunità di effettuare la comunicazione, nonché le relative modalità di comunicazione dei predetti dati, per la quale può essere richiesto un contributo a copertura dei costi sostenuti.
5. 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.
6. 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.
7. L'Università, al fine di agevolare l'orientamento, le esperienze formative e professionali e l'eventuale collocazione nel mondo del lavoro, anche all'estero, può comunicare o diffondere, anche su richiesta di soggetti privati e per via telematica, dati ed elenchi riguardanti studentesse/studenti, diplomate/i, laureande/i e laureate/i, specializzate/i, borsisti, dottorande/i di ricerca 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.
8. L'Università può comunicare altresì, a finanziatori di borse di studio e dottorato di ricerca anche stranieri, dati comuni relativi a borsisti e dottorandi che abbiano usufruito dei finanziamenti.
9. 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.
10. 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.
11. L'Università può comunicare, ad enti pubblici o privati che organizzano e gestiscono corsi di formazione, i dati comuni del personale che partecipa a tali corsi.

## Articolo 33 - Comunicazione e diffusione di dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico l'Università può comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei dati di cui agli articoli 17 e 18.
2. I dati di cui al precedente articolo non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241 e possono essere trattati per i soli scopi in base ai quali sono comunicati o diffusi.
3. L'Università può comunicare eventuali informazioni inerenti 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:

a) promuovere modelli di programmazione delle attività di ricerca e di allocazione delle risorse secondo meccanismi che consentano di garantire trasparenza nella definizione delle priorità, di valorizzare adeguatamente le capacità dei singoli e dei gruppi e di rispettare i principi di trasparenza ed equità di trattamento;

b) favorire la cooperazione tra singoli e gruppi mediante una precisa conoscenza dei risultati conseguiti, allo scopo di migliorare la capacità di attrarre finanziamenti esterni o di istituire forme di collaborazione strutturata con soggetti terzi;
c) fornire orientamento e sostegno per lo sviluppo di modelli organizzativi di supporto alla ricerca, anche tramite la realizzazione di analisi comparative e la condivisione di buone pratiche.

4. L'Università può comunicare dati personali a soggetti pubblici che abbiano erogato dei finanziamenti per la ricerca, ai fini di rendicontazione e per consentire elaborazioni statistiche.

### Articolo 34 - Diffusione delle valutazioni d'esame

1. In ottemperanza ai principi di trasparenza cui l'Università si ispira e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, è consentita la pubblicazione dei dati inerenti alle valutazioni d'esame anche sui siti web di Ateneo.
2. La pubblicazione dei dati sui siti web è consentita mediante la diffusione del numero di matricola dello studente e del voto conseguito, nel rispetto del principio di minimizzazione e dei diritti e delle libertà fondamentali dell'interessato.
3. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a tre mesi.

### Articolo 35 - Diffusione dei risultati di concorsi e selezioni

1. In ottemperanza ai principi di trasparenza cui l'Università si ispira, fermi restando gli altri obblighi di pubblicità legale, sono pubblicati, anche sui siti web di Ateneo, i bandi di concorso per il reclutamento, a qualsiasi titolo, di personale presso l'amministrazione, nonché i criteri di valutazione della Commissione, le tracce delle prove e le graduatorie finali, aggiornate con l'eventuale scorrimento degli idonei non vincitori.
2. La pubblicazione dei dati sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati.

### Articolo 36 - Diffusione dei dati nel pubblico interesse

1. La divulgazione di risultati scientifici contenenti dati personali, se di rilevante interesse pubblico o sociale, non si pone in contrasto con il rispetto della sfera privata se l'interessato sia stato adeguatamente informato in merito alla diffusione di proprie informazioni.

## TITOLO VII
## DISPOSIZIONI FINALI

### Articolo 37 - Disposizioni finali e norme di rinvio

1. Per quanto non espressamente previsto dal presente regolamento si rinvia alle disposizioni del Regolamento (UE) 2016/679 e del vigente Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di

indirizzo e dalle regole deontologiche adottate e approvate dal Garante per la protezione dei dati personali.

### Articolo 38 - Entrata in vigore, pubblicità e revisione

1. Il presente regolamento è approvato dal Consiglio di Amministrazione ed è emanato con Decreto Rettorale.
2. Il Regolamento è pubblicato sul sito istituzionale di Sapienza, nella sezione “Regolamenti”, nonché sulla pagina web dell’Area Affari Legali entro il primo giorno lavorativo successivo alla data di emanazione ed entra in vigore il quindicesimo giorno successivo alla data di emanazione.
3. Dalla data di entrata in vigore del presente Regolamento sono abrogate tutte le disposizioni precedenti, con esso incompatibili.
4. Il presente regolamento è soggetto a revisione nel caso in cui si rende necessario un adeguamento alla normativa vigente in materia di protezione dei dati.