IL RETTORE

Visto lo Statuto;

Visto il Regolamento UE n. 679 del 27 aprile 2016;

Visto il d.lgs. 196/2003, recante il "Codice in materia di protezione dei dati personali", come novellato dal d.lgs. 101/2018;

VISTA la delibera n. 06/01 del 19 dicembre 2025 del Senato Accademico;

VISTA la delibera n. 08/02 del 29 gennaio 2026 del Consiglio di Amministrazione;

DECRETA

di emanare il seguente Regolamento di Ateneo in materia di protezione dei dati personali:

Regolamento di Ateneo in materia di protezione dei dati personali

TITOLO I
DISPOSIZIONI GENERALI

Articolo 1 - Ambito di applicazione

1. Il presente Regolamento, adottato in attuazione del Regolamento (UE) 27 aprile 2016, n. 679 (in seguito Regolamento UE) e del d.lgs. n. 196/2003 come novellato dal d.lgs. n. 101/2018 (in seguito Codice in materia di protezione dei dati personali), disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi all'interno dell'Università degli Studi di Palermo.
2. L'Università, in qualità di titolare del trattamento, effettua i trattamenti di dati con o senza ausilio di processi automatizzati.
3. I dati sono trattati nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.
4. L'Università considera il trattamento lecito, corretto e trasparente dei dati personali un'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, devono effettuare il trattamento secondo la politica di protezione dei dati personali stabilita dal presente Regolamento.

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 ("interessato"); 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**: si tratta dei dati c.d. sensibili, idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'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;
   d. **dati giudiziari**: dati idonei a rivelare l'esistenza, a carico dell'interessato, di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o di indagato. L'art. 10 del Regolamento (UE) 2016/679 ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
   e. **dati personali comuni**: dati personali che non appartengono alle categorie particolari di dati personali e non sono relativi a condanne penali e a reati o a connesse misure di sicurezza;
   f. **dati genetici**: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona stessa;
   g. **dati biometrici**: 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;
   h. **dati relativi alla salute**: 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;
   i. **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;

j. **contitolare**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altro/i titolare/i del trattamento, determina le finalità e i mezzi del trattamento dei dati personali;
k. **responsabile per la protezione dei dati /data protection officer** (di seguito RPD o DPO): figura specializzata nel supporto al titolare del trattamento, prevista come obbligatoria negli enti pubblici;
l. **responsabile 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;
m. **designati al trattamento**: i responsabili delle strutture di Ateneo nell'ambito della quale i dati personali sono gestiti per le finalità istituzionali, individuati sulla base delle competenze attribuite alla funzione organizzativa o alla carica istituzionale che ricopre;
n. **referenti per la protezione dei dati**: figure che hanno il compito di supportare il designato in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il DPO e con l'ufficio dell'Amministrazione competente in materia di protezione dei dati personali per tutte le attività relative alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia;
o. **responsabile della transizione al digitale**: figura i cui compiti sono definiti dall'art. 17, c. 1-*sexies* del Codice dell'Amministrazione Digitale (CAD), emanato con d.lgs. n. 82 del 7 marzo 2005, e ss.mm.ii.;
p. **responsabile della conservazione dei documenti informatici**: figura i cui compiti sono definiti dall'art. 44 del Codice dell'Amministrazione Digitale e ss.mm.ii.;
q. **amministratore di sistema**: figura professionale individuata nell'ambito informatico, 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 *Enterprise Resource Planning* (ERP) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
r. **autorizzati al trattamento**: le persone fisiche formalmente autorizzate e istruite ad accedere ai dati personali e trattare gli stessi sotto l'autorità diretta e secondo le istruzioni del titolare e/o del designato e per le finalità stabilite dal titolare (artt. 4, 29, 32, 39 del Regolamento UE);
s. **interessato al trattamento**: la persona fisica a cui si riferiscono i dati personali; ovvero la persona fisica, identificata o identificabile, 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;
t. **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;

u. **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 designato e gli autorizzati al trattamento dei dati personali;
v. **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;
w. **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;
x. **processo decisionale automatizzato**: decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti nella sfera giuridica dell'Interessato o che incidono in modo analogo significativamente sullo stesso;
y. **pseudonimizzazione**: il trattamento dei dati personali in modo tale che non possano più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
z. **dato anonimo**: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
aa. **limitazione di trattamento**: il contrassegno dei dati personali, conservati con l'obiettivo di limitarne il trattamento in futuro;
bb. **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;
cc. **registro attività di trattamento**: elenco dei trattamenti di dati, in forma cartacea o digitale, effettuati dal titolare e dal responsabile del trattamento, sotto la loro responsabilità, per la protezione secondo le rispettive competenze;
dd. **valutazione d'impatto sulla protezione dei dati (DPIA)**: 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;
ee. **violazione dei dati personali o data breach:** la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
ff. **rappresentante**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta

per quanto riguarda gli obblighi rispettivi ai sensi del Regolamento UE sulla protezione dei dati personali;

gg. **autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE 679/2016: per l'Italia il Garante per la protezione dei dati personali;

hh. **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;

ii. **comunicazione**: attività che consiste nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione Europea, dal designato e dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

jj. **diffusione**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Articolo 3 - Principi generali

1. Il trattamento dei dati personali viene effettuato dall'Università in applicazione dei principi previsti dall'art. 5 del Regolamento UE, dal Codice in materia di protezione dei dati personali e secondo quanto indicato ai successivi commi 2 e 3.
2. In particolare, i dati personali trattati dall'Università, sono:
   a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
   b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità (limitazione della finalità); un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
   c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
   d. esatti e, se necessario, aggiornati; a tal fine sono adottate le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati (esattezza);
   e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, a condizione dell'attuazione di misure tecniche

e organizzative adeguate richieste dal Regolamento UE (limitazione della conservazione);
   f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale, compresa la protezione, mediante misure tecniche e organizzative adeguate (integrità e riservatezza).
3. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto del contesto e delle finalità del trattamento, l'Università adotta misure tecniche e organizzative adeguate in grado di comprovare il rispetto dei principi di cui al presente Regolamento (responsabilizzazione). A tal fine, ciascuna struttura dell'Università deve:
   a. individuare e implementare, con la collaborazione del titolare del trattamento, del DPO e dell'ufficio dell'Amministrazione competente in materia di protezione dei dati personali le predette misure tecniche e organizzative;
   b. vigilare, unitamente ai predetti soggetti, sul rispetto delle stesse;
   c. predisporre, ove necessario, la valutazione d'impatto ai sensi dell'art. 35 del Regolamento UE.

Articolo 4 - Base giuridica del trattamento

1. L'Università è una pubblica amministrazione ai sensi dell'art. 1, c. 2 del d.lgs. 165/2001 e ss.mm.ii, persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche.
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 Regolamento UE, ovvero nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
3. Come previsto dall'art. 2-*ter*, comma 1, del d.lgs. 196/2003, 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 esclusivamente da una norma di legge o di regolamento o da atti amministrativi generali.
4. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato (principio di necessità).
5. Salvo quanto previsto per le categorie particolari di dati personali di cui al successivo art. 13, il ricorso al consenso dell'interessato costituisce base giuridica residuale ed è ammesso per l'esecuzione di trattamenti facoltativi e ulteriori rispetto alle finalità istituzionali perseguite dall'Ateneo. Tali trattamenti, a titolo puramente esemplificativo, possono comprendere:
   a. diffusione di fotografie, video o altri contenuti multimediali raffiguranti l'interessato su siti web, canali social o materiali informativi dell'Ateneo per finalità promozionali;
   b. adesione a community di alumni, gruppi di interesse, reti professionali o associazioni promosse dall'Ateneo, ma non necessarie allo svolgimento delle attività istituzionali;

c. partecipazione a iniziative di placement, orientamento, mobilità internazionale, mentoring, career coaching o altri servizi che comportino la comunicazione di dati personali a soggetti terzi o partner privati;
d. partecipazione a studi, survey o progetti di ricerca promossi da soggetti terzi o partner privati che richiedano la comunicazione di dati personali di studenti o del personale universitario;
e. partecipazione a eventi, workshop, attività culturali, sportive o ricreative che comportino la raccolta e la comunicazione di dati personali oltre quanto strettamente necessario all'organizzazione dell'evento;
f. comunicazione di dati personali a partner commerciali per l'accesso a sconti, agevolazioni o servizi opzionali (ad esempio, convenzioni con enti privati, palestre, servizi assicurativi);
g. invio di newsletter, materiale informativo e promozionale relativo a iniziative non rientranti nei compiti istituzionali dell'Ateneo;
h. monitoraggio dei percorsi professionali, tramite partecipazione a indagini statistiche o rilevazioni occupazionali che possono richiedere uno specifico consenso in relazione alle modalità operative adottate dall'Ateneo.

Qualora il consenso dell'interessato costituisca base giuridica idonea per il trattamento dei dati personali, ai sensi dell'art. 6, paragrafo 1, lettera a) del Regolamento UE, occorre osservare i seguenti principi generali definiti dal medesimo Regolamento:

a. per essere considerato valido, il consenso deve consistere in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, attraverso una dichiarazione o un'azione positiva inequivocabile, al trattamento dei propri dati personali;
b. il titolare deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali per tutto il periodo nel quale lo stesso viene effettuato. Al termine dell'attività di trattamento la prova del conferimento del consenso deve essere conservata per il tempo strettamente necessario all'adempimento di un obbligo giuridico, cui è soggetto il titolare, o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, ai sensi dell'art. 17, paragrafo 3, del Regolamento UE;
c. il consenso deve essere espresso in relazione a una o più specifiche finalità e l'interessato deve poter scegliere in relazione a ciascuna di esse;
d. il consenso deve essere basato sulle informazioni, di cui agli artt. 13 e 14 del Regolamento UE, fornite all'interessato in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro;
e. non configurano forme di consenso valido il silenzio, l'inattività o l'utilizzo di form precompilati e caselle preselezionate;
f. l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è adeguatamente informato di tale diritto e delle sue modalità di esercizio. Il consenso è revocato con la stessa facilità con cui è accordato;
g. il consenso dell'interessato deve essere esplicito nel caso di trattamenti che riguardino categorie particolari di dati personali, nel caso di processi decisionali

automatizzati, compresa la profilazione, nel caso di trasferimenti di dati verso paesi terzi od organizzazioni internazionali in assenza di garanzie adeguate, ai sensi rispettivamente degli artt. 9, 22 e 49 del Regolamento UE.

TITOLO II
ORGANIGRAMMA DELLA PROTEZIONE DATI

Articolo 5 - Titolare del trattamento

1. Il titolare del trattamento dei dati è l'Università degli Studi di Palermo, intesa come persona giuridica, legalmente rappresentata dal Rettore pro tempore.
2. Il titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del Regolamento UE.
3. Il titolare del trattamento adotta misure tecniche e organizzative adeguate a garantire e 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. Tali misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli da 15 a 22 del Regolamento UE.
4. Le misure tecniche ed organizzative sono periodicamente riesaminate e aggiornate.
5. Nel caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, l'Università assicura che non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento UE trasferendo i dati personali a paesi terzi o organizzazioni internazionali definiti dalla Commissione Europea sulla base di una decisione ai sensi dell'art. 45 del Regolamento UE. In mancanza, potrebbe trasferire dati personali ad un paese terzo o ad una organizzazione internazionale fornendo garanzie adeguate che permettano il riconoscimento di diritti azionabili e mezzi di ricorso effettivi. Qualora non sussistano le condizioni precedentemente elencate il trasferimento è ammesso esclusivamente nelle fattispecie previste all'art. 49 del Regolamento UE.
6. L'Università è tenuta a cooperare con il Garante per la protezione dei dati personali, così come disposto dagli artt. 157-160 del Codice in materia di protezione dati personali.

Articolo 6 - Contitolare

1. Ai sensi dell'art. 26 del Regolamento UE, è possibile che più soggetti condividano la titolarità al trattamento dei dati, qualora insieme definiscano finalità e mezzi del trattamento nonché provvedano congiuntamente ad adottare le misure di protezione adeguate.

2. La contitolarità può essere attuata e definita attraverso un contratto o una convenzione, definendo nello schema negoziale le reciproche responsabilità e dandone chiara e trasparente informazione agli interessati (artt.13 e 14 del Regolamento UE).
3. L'Università e il contitolare del trattamento determinano in modo trasparente, mediante apposito accordo, 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.
4. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
5. Il titolare può delegare la sottoscrizione degli accordi di contitolarità.
6. L'interessato può esercitare i propri diritti nei confronti di ciascun contitolare del trattamento.

Articolo 7 - Responsabile della protezione dei dati personali o data protection officer (RPD o DPO)

1. L'Università, in qualità di ente pubblico, ha l'obbligo di nominare, ai sensi dell'art. 37 del Regolamento UE un responsabile della protezione dei dati (in seguito RPD o DPO).
2. Il DPO è figura specializzata nel supporto al titolare in materia di trattamento dati personali e svolge la funzione di raccordo con il Garante per la protezione dei dati personali e di garante per i soggetti interessati.
3. Il DPO è individuato, tra soggetti con formazione giuridica, in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti.
4. Il 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 a seguito procedura di evidenza pubblica secondo il vigente codice degli appalti.
5. Il DPO è nominato, nel caso di soggetti interni, con decreto del Rettore.
6. Il DPO è tenuto a svolgere i seguenti compiti:
   a. informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché dalla normativa comunitaria e nazionale relativa alla protezione dei dati;
   b. sorvegliare sulle politiche del titolare del trattamento, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c. sorvegliare l'osservanza degli obblighi derivanti dal Regolamento UE, dalla normativa comunitaria e nazionale relativa alla protezione dei dati personali e dai Regolamenti di Ateneo;
   d. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne l'effettivo svolgimento e completamento;
   e. segnalare al titolare ed al Direttore Generale le priorità di intervento in relazione alle novità normative e tecniche e le eventuali inadempienze emerse in occasione dell'espletamento delle funzioni istituzionali;

f. cooperare con il Garante per la protezione dei dati personali;
g. fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
h. collaborare nella redazione e nell'aggiornamento dei registri di trattamento;
i. svolgere ogni ulteriore compito attribuito dal titolare.

7. Il titolare, i designati o loro referenti, i responsabili del trattamento assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   - il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
   - il DPO riceve tempestivamente dal titolare, dai designati o loro referenti e dai responsabili del trattamento le informazioni inerenti le decisioni che incidono significativamente sulla protezione dei dati personali, anche al fine di prestare idonea consulenza;
   - il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tali decisioni;
8. Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
9. Al DPO sono garantiti, supporto, risorse umane e finanziarie e tempi di lavoro adeguati allo svolgimento della sua funzione. Per lo svolgimento dei propri compiti il DPO può avvalersi di uno *staff* costituito dall'Amministrazione, composto da personale con formazione multidisciplinare e comprovata esperienza professionale in ambiti correlati alla *privacy* e alla *data protection*, quali la dematerializzazione documentale, l'analisi dei processi, la trasparenza amministrativa, la comunicazione *on line* e l'accessibilità *web*, la sicurezza informatica e l'analisi del rischio. A seconda della necessità, il DPO può inoltre avvalersi di professionalità interne o esterne all'Ateneo. È garantita, altresì, una formazione permanente specialistica che gli consenta un costante aggiornamento sugli sviluppi nel settore della protezione dei dati.
10. Il DPO ha libero accesso alle informazioni necessarie per svolgere i propri compiti ed è interpellato per ogni problematica inerente la protezione dei dati e per le attività che implicano un trattamento dati, fin dalla loro progettazione.
11. L'Università garantisce che il 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 con la sua posizione. La figura del DPO non può coincidere con quella del Responsabile per la Prevenzione della Corruzione e della Trasparenza.
12. Il DPO non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del Regolamento UE, né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

13. L'Università non rimuove o penalizza il DPO in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni. Le funzioni del DPO cessano per dimissioni o scadenza del mandato se previamente determinato, mentre eventuale revoca deve essere adeguatamente motivata.
14. Il nominativo e i dati di contatto del DPO sono comunicati al Garante per la protezione dei dati personali. I dati di contatto del DPO sono inseriti nelle informative privacy e pubblicati sul sito internet istituzionale.
15. Su indicazione del DPO possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali.
16. Il DPO può nominare un proprio delegato che lo sostituisce in caso di assenza o impedimento. Il delegato deve possedere le competenze necessarie in materia di protezione dei dati e non deve trovarsi in conflitto di interessi. La nomina del delegato del DPO deve essere comunicata al titolare del trattamento.
17. Il DPO redige una relazione annuale dell'attività svolta.

Articolo 8 - Responsabile del trattamento dei dati personali

1. Responsabile del trattamento è qualunque soggetto esterno che esegue, in base a un contratto, convenzione o altro atto giuridico, trattamenti di dati personali per conto dell'Università e ne risponde in solido con l'Università in caso di inadempienze.
2. Il responsabile del trattamento, nominato con atto giuridico conforme al diritto nazionale e all'art. 28 del Regolamento UE, deve fornire idonee garanzie, soprattutto in relazione alle misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni del medesimo Regolamento.
3. L'atto di nomina del responsabile 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. Il titolare può delegare la nomina del responsabile del trattamento e può integrare o precisare, anche successivamente all'atto di nomina, le istruzioni iniziali impartite al responsabile.
5. Previa adeguata integrazione da parte dell'Amministrazione centrale del personale tecnico amministrativo dedicato ed erogazione di adeguate e specifiche attività di formazione dello stesso, i Direttori dei Dipartimenti, dei Centri e i Presidenti delle Scuole di Ateneo nominano i responsabili che eseguono trattamenti di dati personali riconducibili alle strutture di loro competenza. Qualora il trattamento dei dati personali interessi più Dipartimenti o Centri, la nomina spetta congiuntamente ai relativi Direttori o Presidenti.
6. Il responsabile del trattamento può nominare mediante contratto o altro atto giuridico sub-responsabili per specifiche attività di trattamento, previa autorizzazione scritta del titolare. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica prima di ricorrere al sub-responsabile, unitamente alle informazioni necessarie per consentire al titolare di decidere in merito all'autorizzazione.
7. Il responsabile risponde dinanzi all'Università dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

8. Le strutture di Ateneo devono tempestivamente comunicare al DPO e all'ufficio dell'Amministrazione competente in materia di protezione dei dati personali la stipula o l'esistenza di un contratto, convenzione o altro atto giuridico di cui al comma 1 del presente articolo, inviando al contempo la relativa documentazione.

Articolo 9 - Designati al trattamento dei dati personali

1. Sono individuati quali designati al trattamento dei dati personali, sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono, i responsabili delle strutture nell'ambito della quale i dati personali sono gestiti per le finalità istituzionali.
2. L'incarico di designato al trattamento dei dati, di norma, si intende conferito e produce effetti giuridici a decorrere dalla data di nomina alla funzione istituzionale di Direttore di Dipartimento o di Centro, Presidente di Scuola, Direttore Generale o Dirigente, con riferimento alle competenze e responsabilità connesse all'incarico stesso.
3. I designati 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 Aree per le rispettive attività di competenza;
   - per le attività di didattica e di ricerca: i Direttori dei Dipartimenti e dei Centri Interdipartimentali, i Presidenti delle Scuole; per i progetti di ricerca i responsabili/referenti scientifici del progetto, i responsabili di altre tipologie di strutture.
4. Il designato può delegare a un proprio referente strutturato, docente o tecnico amministrativo, tutti i compiti, o parte di essi, di cui al successivo comma 5, relativamente ai diversi ambiti di competenza. La delega, formalizzata con apposito atto, contiene puntualmente i compiti delegati ed è corredata dalle relative istruzioni e dalla individuazione delle modalità di verifica e di controllo. Di tale delega è data: comunicazione al Rettore, al responsabile della protezione dei dati e all'ufficio dell'Amministrazione competente in materia di protezione dei dati personali; evidenza nel registro dei trattamenti e ampia diffusione all'interno dell'amministrazione (rete intranet, ufficio personale ecc.).
5. Il designato o suo referente, opportunamente formato riguardo alle competenze anche decisionali in materia di protezione dei dati, opera con autonomia gestionale nell'ambito delle competenze affidategli, collabora funzionalmente con il DPO per l'espletamento dei compiti e per gli ambiti espressamente definiti all'interno della propria struttura di afferenza assegnategli dal titolare con formale incarico.
6. I designati, nei limiti dei poteri e delle funzioni rientranti nella natura della posizione ricoperta:
   a. coadiuvano il titolare nella definizione delle finalità e delle modalità di trattamento;
   b. collaborano con il titolare nell'individuare i mezzi idonei a garantire l'osservanza della normativa sulla privacy;

c. sovraintendono alle attività di trattamento dei dati;
d. garantiscono il rispetto della normativa privacy e del presente regolamento;
e. controllano la corretta esecuzione da parte dei referenti/incaricati delle istruzioni per il trattamento dei dati personali.

7. I designati al trattamento si attengono alle istruzioni dell'Università, o del diverso titolare che ha designato l'Università quale responsabile del trattamento, e, in particolare, si impegnano a:
   a. istruire i referenti/incaricati, che svolgono funzioni all'interno della propria struttura, sulla normativa privacy e sul presente regolamento per garantirne la corretta applicazione;
   b. verificare che soltanto i referenti/incaricati che hanno ricevuto le adeguate istruzioni possano accedere alle operazioni di trattamento dei dati;
   c. segnalare tempestivamente carenze delle vigenti misure organizzative e tecniche finalizzate alla protezione dei dati personali;
   d. assicurare che per ogni trattamento in essere sia stata individuata la corretta base giuridica;
   e. assicurare che gli accordi con i responsabili esterni all'Università (es. fornitori, partner, ecc.) contengano le disposizioni necessarie in conformità a quanto indicato all'art. 28 del Regolamento UE;
   f. predisporre, per i trattamenti che hanno come base giuridica il consenso, 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;
   g. assicurare, anche tramite i loro referenti, che i nuovi trattamenti effettuati dalla propria struttura siano inseriti nel registro dei trattamenti documentando e segnalando al titolare, e in conoscenza al DPO e all'ufficio dell'Amministrazione competente in materia di protezione dei dati personali, il censimento periodico dei trattamenti in atto;
   h. comunicare al titolare, e per conoscenza al DPO e all'ufficio dell'Amministrazione competente in materia di protezione dei dati personali, l'intenzione di avviare nuovi trattamenti che, prevedendo l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, potrebbero presentare un rischio elevato per i diritti e le libertà degli interessati, affinché il DPO possa fornire il proprio parere sulla valutazione di impatto;
   i. riscontare le richieste degli interessati entro il termine di giorni 30 (trenta) dalla ricezione.
8. Nel caso in cui, presso la struttura di riferimento, siano presenti sistemi di videosorveglianza, il designato è delegato dal titolare a svolgere specifiche funzioni espressamente definite con apposito atto, in conformità a quanto disposto dal successivo articolo 19 del presente regolamento e del vigente regolamento per la gestione dei dati tramite il sistema di videosorveglianza.

Articolo 10 - Autorizzati al trattamento dei dati personali

1. Gli autorizzati al trattamento sono formalmente nominati dal designato, o suo referente, tra il personale docente e tecnico amministrativo e operano sotto la sua diretta autorità.

Tali autorizzazioni sono registrate e periodicamente aggiornate nella piattaforma di gestione degli incarichi all'uopo dedicata.

2. Gli autorizzati al trattamento ricevono opportuna formazione/informazione specifica in materia di trattamento dei dati personali.
3. Nelle more della nomina formale e individuale di incaricati del trattamento dati, coloro che trattano dati che competono alla unità organizzativa cui afferiscono, sono ritenuti autorizzati al trattamento dei dati per formale preposizione ad unità organizzativa e pertanto sono obbligati ad osservare quanto previsto dal presente articolo.
4. L'autorizzato effettua i trattamenti dei dati personali in osservanza delle misure di sicurezza previste dall'Università, finalizzate ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati personali.
5. L'autorizzato è tenuto:
   - a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante l'attività prestata;
   - a non comunicare a terzi o diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di autorizzato;
   - a seguire i seminari d'informazione e formazione in materia di protezione dei dati personali e a sostenere i relativi test finali per la verifica dell'apprendimento;
   - a segnalare con tempestività al proprio responsabile di ufficio, al designato o referente eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati (*data breach*) al Garante per la protezione dei dati personali e ai soggetti interessati;
6. L'autorizzato è tenuto ad effettuare i trattamenti secondo le istruzioni dettagliate nell'atto di nomina dal designato della struttura di afferenza, sotto la propria responsabilità e in relazione a specifici compiti e funzioni connessi al trattamento dati e in ogni caso a rispettare quanto previsto dalla normativa in materia di trattamento dei dati personali e dai provvedimenti dell'Autorità Garante;
7. L'autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici aziendali per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari, oltre che esporre l'amministrazione a danni reputazionali, oltre che patrimoniali.
8. L'autorizzato si impegna a osservare le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica e logica adottate dall'Università.
9. Nel caso in cui non ricorrano le condizioni di cui al presente articolo, coloro che, nello svolgimento dei propri compiti, vengano a conoscenza di dati personali per i quali non possiedono esplicita autorizzazione al trattamento o che non competono alla unità organizzativa cui afferiscono, sono considerati come terzi rispetto all'amministrazione stessa, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.
10. L'autorizzato al trattamento di dati raccolti mediante impianti di videosorveglianza è formalmente nominato dal designato, o suo referente, tra il personale docente e tecnico amministrativo e opera sotto la sua diretta autorità, riceve opportuna

formazione/informazione specifica in materia di trattamento dati raccolti mediante impianti di videosorveglianza, si attiene a quanto disposto dal successivo articolo 19 del presente regolamento, dal vigente regolamento per la gestione dei dati tramite il sistema di videosorveglianza e a quanto contenuto nello specifico incarico ricevuto.

Articolo 11 - Amministratori di Sistema

1. L'Amministratore di Sistema (in seguito AdS), così come definito al precedente articolo 2, è una figura professionale che può ricoprire presso l'Università i seguenti ruoli:
   - amministratore delle basi di dati (*database administrator*), responsabile dell'integrità dei dati stessi, dell'efficienza e delle prestazioni del sistema-database;
   - amministratore della rete (*network administrator*) che gestisce l'infrastruttura di rete (apparati come hub, switch e router) ed effettua le diagnosi dei problemi che i vari personal computer o server hanno con essa;
   - amministratore della sicurezza (*security administrator*), compresa la gestione dei dispositivi tipo firewall e l'adozione di misure di sicurezza generale;
   - amministratore web (*web administrator*), che si preoccupa della gestione dei servizi web, ovvero servizi che permettono ad utenti interni o esterni di accedere ai siti web;
2. Non rientrano in questa categoria quei soggetti che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software per scopi di manutenzione a seguito di guasti o malfunzionamenti.
3. Le principali funzioni dell'AdS comportano un'effettiva capacità di azione sulle informazioni, contenute all'interno del sistema informatico, tanto da poter costituire a tutti gli effetti un trattamento di dati personali, anche quando le informazioni non sono consultabili "in chiaro".
4. Il titolare del trattamento dei dati o i designati, preposti a strutture che ne abbiano necessità, possono nominare uno o più AdS, specificando gli elaboratori, le reti, gli applicativi complessi o le banche dati che sono chiamati a sovrintendere, informandoli delle responsabilità che sono loro affidate in relazione a quanto disposto dalle normative in vigore.
5. Per procedere all'attribuzione delle funzioni di AdS, devono essere valutate preventivamente le caratteristiche personali e professionali del soggetto, che deve possedere requisiti di esperienza, capacità e affidabilità, nonché dare garanzia del rispetto, oltre che della conoscenza, delle disposizioni in materia di trattamento dei dati personali, sicurezza compresa. Gli stessi sono tenuti ad informarsi ed aggiornarsi al riguardo, anche mediante la partecipazione agli incontri e seminari formativi che vengano in materia organizzati dal titolare.
6. La designazione individuale dell'AdS deve seguire un preciso profilo di autorizzazione, mediante affidamento di specifici ambiti di operatività e evitando ogni accesso a dati eccedenti rispetto le necessità della sua azione.
7. L'atto di incarico deve contenere:
   - l'attestazione che l'incaricato ha le caratteristiche richieste;
   - l'elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato;

- l'indicazione delle verifiche almeno annuali che il titolare o il responsabile delegato dovranno svolgere sulle attività svolte dell'amministratore di sistema;
- l'indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed eventualmente a terzi nei modi richiesti dalla normativa vigente.

8. L'atto di incarico deve essere controfirmato dall'interessato per presa visione e accettazione.
9. Gli estremi identificativi delle persone fisiche che ricoprono il ruolo di AdS sono contenuti in un elenco in cui vengono indicate le funzioni loro attribuite. Il predetto elenco, atteso che tali figure trattano anche dati relativi ai lavoratori, è pubblicato nell'intranet di Ateneo e inviata all'ufficio dell'Amministrazione competente in materia di protezione dei dati personali, al Servizio che cura le relazioni sindacali e al DPO.
10. L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei designati, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti e dai regolamenti di Ateneo.

TITOLO III
TRATTAMENTO DEI DATI PERSONALI

Articolo 12 - Tipologie di dati personali

1. L'Università 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 Regolamento UE, del Codice in materia di protezione dei dati personali, nonché delle Linee guida e dei provvedimenti del Garante per la protezione dei dati personali.
2. I trattamenti dei dati personali avvengono secondo le modalità e per le finalità descritte al precedente articolo 3 e possono riguardare, a titolo esemplificativo e non esaustivo:
   a. dati, anche di natura particolare, relativi al personale con rapporto di lavoro dipendente o con rapporto di lavoro autonomo o con altre tipologie contrattuali previste dalla legge, ivi compresi, i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nell'Università. A titolo esemplificativo e non esaustivo si indicano i dati inerenti a:
      - prove concorsuali/selezioni;
      - gestione del rapporto di lavoro;
      - formazione e aggiornamento professionale;
      - politiche welfare e per la fruizione di agevolazioni;
      - salute e sicurezza delle persone nei luoghi di lavoro;
      - erogazione del servizio di telefonia fissa e mobile;
   b. dati che riguardano gli studenti, per tutte le attività e modalità connesse alla qualità di studente, inteso nella accezione più ampia, ivi compresi laureati, dottorandi di

ricerca, specializzandi, tirocinanti e studenti iscritti presso altre Università, anche straniere, che frequentano l'Ateneo a qualunque titolo per fini didattici e/o di ricerca. A titolo esemplificativo e non esaustivo si indicano i dati inerenti a:
- attività di orientamento;
- erogazione dei test di ingresso o alla verifica dei requisiti di accesso;
- erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea);
- attività di tirocinio;
- attività di job placement;
- attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community;
- rilevazioni statistiche e valutazione della didattica;
- diffusione dell'elaborato finale o di elementi ad esso connessi;
- servizi di tutorato, assistenza, inclusione sociale;
- servizi e attività per il diritto allo studio;
- procedimenti di natura disciplinare a carico di studenti;

c. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi alla didattica e alla ricerca, compresa la ricerca in ambito medico e sanitario, quali ad esempio:
   - dati particolari e giudiziari trattati nell'ambito delle attività di ricerca inerenti *in toto* le scienze tecniche, scienze mediche e scienze umanistiche, scienze della formazione;
   - dati particolari trattati nell'ambito delle attività didattiche e assistenziali connesse alla ricerca;
   - dati inerenti lo stato di salute acquisiti nell'ambito delle strutture ospedaliere e sanitarie convenzionate.

d. dati personali, anche di natura particolare, con riferimento a determinati servizi relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali; quali quelli inerenti, a titolo esemplificativo e non esaustivo:
   - gestione degli spazi;
   - gestione delle postazioni;
   - gestione degli organi e delle cariche istituzionali;
   - gestione degli infortuni;
   - servizi bibliotecari;
   - servizi di protocollo e conservazione documentale;
   - acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso;
   - servizi di posta elettronica e strumenti di collaborazione;
   - erogazione federata di servizi;
   - erogazione del servizio *Eduroam*;
   - accesso a servizi federati;
   - accesso ai servizi con autenticazione SPID;
   - tracciamento di informazioni non primarie;

e. dati relativi alla gestione del contenzioso giudiziale, stragiudiziale e attività di consulenza.

3. È compito dei designati o dei loro referenti aggiornare e documentare il censimento periodico dei trattamenti in atto e segnalare eventuali nuovi trattamenti.
4. Tutti i trattamenti effettuati devono essere inseriti nel registro delle attività di trattamento del titolare di cui all'art. 20 del presente regolamento e costantemente aggiornati.

Articolo 13 - Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, fatti salvi i seguenti casi:
   a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
   b. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
   c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   e. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria 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, a condizione che tali dati siano trattati da o sotto la responsabilità di un professionista soggetto al 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 dell'articolo 89, paragrafo 1, del Regolamento UE, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
   h. il trattamento è necessario per motivi di interesse pubblico rilevante, se previsto dal diritto dell'Unione ovvero, nell'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 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 in materia di protezione dei dati personali.
3. 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, fermo restando quanto previsto dall'art. 2-*septies* del Codice in materia di protezione dei dati personali.

Articolo 14 - Trattamento di dati relativi a condanne penali e reati

1. Il trattamento dei dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza (c.d. dati giudiziari) da parte dell'Ateneo è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati, ai sensi ai sensi dell'art. 10 del Regolamento UE e dell'art. 2-*octies* del Codice in materia di protezione dei dati personali, riguardanti in particolare:
   a. l'adempimento di obblighi e l'esercizio di diritti da parte del titolare del trattamento o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dall'art. 9, c. 2, lett. b), e dall'art. 88 del Regolamento UE;
   b. l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
   c. la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdettivi nei casi previsti dalle leggi o dai regolamenti;
   d. l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa;
   e. l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   f. l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
   g. l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza;
   h. l'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.
   i. l'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.

j. l'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.

2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonché le garanzie di cui al medesimo comma sono individuati con decreto del Ministro della giustizia, ai sensi dell'articolo 2-*octies*, comma 2, del Codice in materia di protezione dei dati personali.

Articolo 15 - Trattamento di dati personali nell'ambito del rapporto di lavoro

1. L'Università effettua il trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi.
2. Il trattamento dei dati relativi ai dipendenti da parte dell'Università non richiede il consenso esplicito in quanto il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
3. L'Università garantisce ai dipendenti l'esercizio dei diritti previsti dagli artt. 12-22 del Regolamento UE, compreso il diritto di accesso ai dati valutativi di natura soggettiva, nonché il diritto all'informativa.
4. L'Università adotta misure tecniche e organizzative atte a garantire la tutela delle prerogative individuali e sindacali come disposte dalla normativa italiana, in particolare dallo Statuto dei lavoratori (Legge 20 maggio 1970, n. 300) e dalle norme che lo richiamano, oltre che dalle regole deontologiche promosse dal Garante per la protezione dei dati personali.
5. 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.
6. 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.
7. 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 16 - Trattamento di dati personali ai fini di archiviazione nel pubblico interesse o di ricerca storica

1. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.
2. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto del principio della minimizzazione dei dati.

3. Ove possibile e senza pregiudicare il raggiungimento delle finalità del trattamento, i dati devono essere trattati con misure tecniche che non consentano più di identificare l'interessato.
4. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità secondo i principi stabiliti dall'articolo 5 del Regolamento UE.
5. Il trattamento dei dati personali per fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto delle garanzie per i diritti e le libertà dell'interessato, in conformità all'art. 89 del Regolamento UE e alle regole deontologiche promosse dal Garante, ai sensi degli artt. 2-*quater* e 102 del Codice in materia di protezione dei dati personali.
6. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42, dalle relative regole deontologiche e dai regolamenti di Ateneo in materia.

Articolo 17 - Trattamento di dati personali ai fini statistici o di ricerca scientifica

1. Il trattamento di dati personali ai fini statistici o di ricerca scientifica, compresa la ricerca medica, biomedica ed epidemiologica, da parte di chiunque operi all'interno di uffici e strutture dell'Università o per conto dell'Università stessa, deve avvenire nel rispetto dei seguenti principi:
   a. i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né trattati per altri scopi;
   b. all'interessato deve essere fornita puntuale informazione, ai sensi degli artt. 13 e 14 del Regolamento UE, 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 di cui all'articolo 106 del Codice in materia di protezione dei dati personali.
   c. il trattamento dei dati personali per fini statistici o di ricerca scientifica è effettuato nel rispetto delle garanzie per i diritti e le libertà dell'interessato, adottando misure tecniche e organizzative idonee (quali pseudonimizzazione, minimizzazione, separazione dei dati identificativi, cifratura), in conformità all'art. 89 del Regolamento UE e alle regole deontologiche promosse dal Garante, ai sensi degli artt. 2-*quater* e 106 del Codice in materia di protezione dei dati personali.
2. Il trattamento dei dati personali deve essere documentato in un progetto conforme agli standard metodologici, contenente finalità, categorie di dati, misure di sicurezza e modalità di conservazione. Il progetto deve essere conservato per almeno cinque anni e reso disponibile all'Autorità di controllo su richiesta.
3. 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.

4. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento UE, 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.
5. Il consenso, per i trattamenti di cui al precedente comma, 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 titolare del trattamento, oltre ad acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca, adotta le misure appropriate individuate dal Garante per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, ai sensi dell'art. 110 del Codice in materia di protezione dei dati personali.
6. 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.
7. 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 18 - Trattamento di dati personali nelle sedute degli Organi collegiali di Ateneo

1. Nel corso delle sedute degli Organi collegiali di Ateneo, il trattamento dei dati correlati agli argomenti in trattazione, comunicati dalle strutture universitarie in qualità di promotrici e referenti dei punti all'ordine del giorno, avviene in conformità alle prescrizioni del Regolamento (UE) 2016/679, del d.lgs. 196/2003, del presente regolamento, nonché delle Linee guida del Garante per la protezione dei dati personali.
2. Le finalità del trattamento di cui al precedente comma sono connesse all'espletamento delle attività istruttorie, da parte dei componenti degli Organi collegiali, per l'adozione delle relative delibere.
3. I dati personali trattati devono essere pertinenti, adeguati e limitati a quanto strettamente necessario rispetto alle finalità perseguite, in conformità al principio di minimizzazione, di cui all'art 5, paragrafo 1, lettera c) del Regolamento UE. È vietata la diffusione di dati personali, in particolare di quelli appartenenti a categorie particolari, salvo che ciò sia espressamente previsto da disposizioni di legge o di regolamento o da atti amministrativi generali per motivi di interesse pubblico rilevante, nel rispetto delle garanzie previste.

Tale divieto si applica all'intero processo istruttorio e deliberativo allo scopo di prevenire trattamenti non autorizzati anche nelle fasi preliminari e interne alle sedute.

4. Ove ravvisino tale necessità, gli Organi collegiali possono consultare il responsabile della protezione dei dati (DPO) per dirimere dubbi interpretativi e operativi legati al corretto trattamento dei dati personali.
5. È obbligatoria la consultazione preventiva del DPO:
   - in caso di deliberazioni che incidano sulla politica di gestione dei dati personali;
   - quando si preveda il trattamento di dati appartenenti a categorie particolari;
   - prima dell'adozione di misure che comportino una valutazione d'impatto sulla protezione dei dati (DPIA), ai sensi dell'art. 35 del Regolamento UE.
6. I verbali delle sedute devono essere redatti nel rispetto del principio di minimizzazione, evitando l'inclusione di dati personali non essenziali. In caso di pubblicazione, devono essere adottate misure di anonimizzazione o oscuramento dei dati non pertinenti, nel rispetto delle norme sulla privacy e la trasparenza amministrativa e secondo quanto previsto dalle Linee guida del Garante per la protezione dei dati personali e dell'Autorità Nazionale Anticorruzione (ANAC).

Articolo 19 - Videosorveglianza

1. L'Università degli Studi di Palermo può installare presso i locali e nelle aree dei quali è titolare sistemi di video sorveglianza, nell'ambito dei propri fini istituzionali, al fine:
   - di garantire il regolare svolgimento delle attività didattiche di ricerca, per garantire la sicurezza e l'incolumità di studenti, utenti, visitatori e di quanti accedono ai propri locali;
   - per tutelare il proprio patrimonio mobiliare e immobiliare contro il rischio di furti e danneggiamenti;
   - per assicurare la sicurezza e la riservatezza dei documenti e dei dati personali in essi contenuti;
   - per l'accertamento e prova di comportamenti illeciti, attuabili ex post in ragione di concreti indizi, (c.d. controlli difensivi, in "senso stretto", a tutela del patrimonio e dell'immagine dell'ente) purché diversi dal mero inadempimento della prestazione lavorativa e, comunque, nel rispetto dei presupposti di legittimità di cui all'art. 4 dello Statuto dei lavoratori.
2. 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.
3. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nel presente regolamento e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria e dell'autorità giudiziaria.
4. 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. Le immagini

raccolte non devono essere in alcun modo impiegate come strumento di sorveglianza a distanza del personale universitario e di tutti coloro che operano a vario titolo in Ateneo, sia con riferimento allo svolgimento dell'attività lavorativa che con riferimento alle proprie abitudini personali. A tale proposito, è vietata l'installazione di videocamere in luoghi esclusivamente destinati allo svolgimento dell'attività lavorativa; in particolare, non potranno essere in alcun caso riprese le apparecchiature di rilevazione automatizzata della presenza del personale.

5. Laddove dai sistemi installati, per le finalità di cui al comma 1, derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, l'Università adotta le garanzie previste dall'art. 4 dello Statuto dei lavoratori, stipulando un accordo collettivo con la rappresentanza sindacale dell'Università ovvero, in mancanza di accordo, previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, qualora siano interessate sedi dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro.
6. La durata della conservazione dei dati raccolti mediante gli impianti di videosorveglianza è limitata entro le 48 (quarantotto) ore lavorative. Le registrazioni effettuate nel pomeriggio del venerdì e nei giorni di sabato e domenica dovranno essere disponibili non oltre le ore 24 del martedì successivo. Lo stesso dovrà avvenire in corrispondenza dei periodi di chiusura prolungata delle strutture di Ateneo, nei quali casi le registrazioni effettuate dovranno essere disponibili non oltre le ore 24 del secondo giorno successivo di apertura. Sono fatte salve speciali esigenze di ulteriore conservazione connesse a festività o periodi di chiusura delle sedi universitarie da definire all'occorrenza con appositi e motivati decreti rettorali, ovvero a specifiche richieste di autorità giudiziaria o polizia giudiziaria, per finalità di prevenzione, accertamento o repressione di reati. Il sistema impiegato deve essere programmato in modo da operare al momento prefissato, ove tecnicamente possibile, la cancellazione automatica da ogni supporto, anche mediante sovra registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
7. Le eventuali modificazioni degli impianti esistenti nonché l'installazione di nuovi impianti potranno avvenire nel rispetto delle norme del presente regolamento, del Codice e dei provvedimenti dell'Autorità Garante in materia, con contestuale comunicazione al DPO e all'ufficio dell'Amministrazione competente in materia di protezione dei dati personali.
8. Nel caso di videosorveglianza svolta con l'utilizzo di sistemi innovativi con telecamere c.d. "intelligenti", è in ogni caso necessario, prima di procedere all'installazione o implementazione:
   a. effettuare la valutazione di impatto per il trattamento che viene svolto tramite il sistema di videosorveglianza intelligente da installare o implementare, in ossequio al disposto di cui all'art. 35, paragrafo 3, lett. c), del Regolamento UE e alle indicazioni contenute nelle Linee guida del Comitato Europeo per la protezione dei dati (EDPB) sul trattamento dei dati personali attraverso dispositivi video;
   b. acquisire il parere del DPO sulla valutazione di impatto sulla protezione dei dati personali (DPIA). Le strutture che, per particolari esigenze debitamente documentate, dovessero avere necessità di installare questa tipologia di impianto devono preventivamente comunicarlo al DPO e all'ufficio dell'Amministrazione

competente. Sarà cura delle stesse strutture procedere all'attivazione della suddetta procedura;

c. 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.

9. In prossimità delle postazioni in cui sono state collocate le telecamere è affissa adeguata e visibile segnaletica permanente contenente l'informativa, che dovrà essere visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.
10. L'Università garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza. In particolare:
    - tutto il personale coinvolto nelle operazioni di registrazione, visualizzazione e registrazione delle immagini, nonché il personale addetto alla manutenzione degli impianti e alla pulizia dei locali riceve una adeguata formazione sui comportamenti da adottare in armonia con quanto previsto dalla normativa vigente in tema di protezione dei dati personali;
    - può avere accesso alle immagini solo il personale autorizzato con specifico atto di nomina;
    - il personale autorizzato è tenuto al segreto professionale;
    - le immagini non possono essere conservate per un periodo più lungo del necessario in conformità con quanto previsto dai principi applicabili al trattamento dei dati personali;
    - nel caso in cui le immagini siano conservate per un periodo maggiore di quello previsto dal regolamento, esse devono essere custodite in un posto sicuro con accesso controllato e cancellate non appena la loro conservazione non sia più necessaria.
11. Il titolare del trattamento, con specifico atto, indica al designato, nel caso in cui nella struttura fosse presente un impianto di videosorveglianza, gli specifici compiti che dovranno essere svolti dallo stesso;
12. È onere del titolare o responsabile della struttura nella quale sono installati strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio:
    a. verificare che siano attuate le prescrizioni stabilite con la valutazione di impatto sulla protezione dei dati (DPIA), appositamente redatta in merito al trattamento in questione;
    b. redigere motivata relazione sulle specifiche esigenze perseguite dall'attività di videosorveglianza all'interno della struttura di riferimento;
    c. verificare che l'installazione e l'uso delle telecamere sia proporzionale al grado di rischio presente in concreto e che le stesse vengano utilizzate in modo da evitare eccessi e ridondanze (gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali

controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi, etc.);

d. individuare e designare gli autorizzati al trattamento dei dati raccolti mediante i sistemi di videosorveglianza, impartendo loro per iscritto le necessarie istruzioni. Tali autorizzazioni devono essere caricate e aggiornate nella piattaforma di gestione degli incarichi all'uopo dedicata;
e. individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini, dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.);
f. verificare, ai sensi del presente regolamento e del vigente regolamento che disciplina l'uso dello specifico impianto adottato, che la durata della eventuale conservazione delle immagini sia limitata a poche ore o, al massimo, alle quarantotto ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione come indicati al comma 6;
g. verificare che i sistemi di videosorveglianza siano installati e vengano usati nel rispetto della normativa sulla sicurezza dei dati personali e di altre disposizioni normative da osservare in caso di installazione di impianti audiovisivi;
h. verificare che, nelle immediate vicinanze delle telecamere posizionate, siano stati collocati dei supporti con l'informativa, visibili in ogni condizione di illuminazione ambientale (anche quando il sistema di videosorveglianza è attivo in orario notturno);
i. adottare e rispettare le misure minime di sicurezza al fine di ridurre al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
j. fornire tempestivo riscontro alle richieste di accesso ai dati raccolti mediante i sistemi di videosorveglianza e ai reclami degli interessati;
k. nel caso in cui l'installazione e/o la manutenzione delle videocamere avvenga ad opera di un soggetto esterno, acquisire da quest'ultimo la descrizione scritta dell'intervento effettuato che ne attesti la conformità alla normativa di riferimento (i soggetti preposti alle predette operazioni possono accedere alle immagini solo in caso di verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitati alla visione delle immagini);
l. qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, verificare che gli stessi siano protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* e ss. c.p..

13. I programmi informatici dovranno essere configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. In particolare, nel rispetto dei principi di pertinenza, non eccedenza e necessità sono da evitare riprese di dettaglio, quali primi piani delle persone, che non siano funzionali rispetto alle finalità istituzionali dell'impianto.
14. L'accesso ai sistemi è consentito esclusivamente al titolare, al responsabile, al designato e agli autorizzati di cui all'art. 12. Ciascuno di essi è dotato delle credenziali di

autenticazione di cui è responsabile per la custodia, la conservazione e la assoluta riservatezza.

15. Il titolare del trattamento, tramite i designati e i responsabili, adotta preventivamente idonee misure di sicurezza al fine di proteggere i dati e ridurre al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.
16. L'interessato, dietro presentazione di apposita istanza, può:
    a. accedere esclusivamente ai dati che lo riguardano;
    b. richiedere informazioni circa le finalità, le modalità e la logica del trattamento;
    c. opporsi, motivatamente, in tutto o in parte al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.
17. Qualora, presso le strutture d'Ateneo, il servizio di videosorveglianza venga erogato da soggetti esterni, gli stessi dovranno essere nominati quali responsabili del trattamento dei dati personali raccolti mediante gli impianti di videosorveglianza con provvedimento del Rettore pro tempore.
18. L'Università degli Studi di Palermo, nel rispetto dei principi del presente regolamento e di quanto prescritto con il presente articolo, provvede a disciplinare, con apposito regolamento, i sistemi di videosorveglianza installati presso le sedi, i locali e le aree di pertinenza della stessa Università.

TITOLO IV
PROTEZIONE E SICUREZZA DEI DATI

Articolo 20 - Registro delle attività di trattamento

1. Il titolare del trattamento dei dati, in applicazione dell'art. 30, paragrafo 1, del Regolamento UE, ha l'obbligo di tenere ed aggiornare un registro delle attività di trattamento svolte sotto la propria responsabilità. Ogni designato è tenuto a monitorare costantemente il registro chiedendone eventualmente l'integrazione con trattamenti di propria competenza.
2. Il registro censisce le attività di trattamento svolte dagli uffici e dalle strutture dell'Università e le principali caratteristiche dei trattamenti. Il registro è costantemente aggiornato, e, su richiesta, messo a disposizione del Garante per la protezione dei dati personali.
3. Il registro dei trattamenti dei quali l'Università è titolare contiene le seguenti informazioni:
    - il nome ed i dati di contatto dell'Università, del DPO, dei designati e dei loro referenti;
    - le strutture competenti al trattamento;
    - le finalità del trattamento;
    - la descrizione delle categorie di interessati, nonché le categorie di dati personali;
    - le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
    - l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

4. Nel caso in cui l'Università svolga il ruolo di responsabile del trattamento dei dati personali, il registro dei trattamenti contiene le seguenti informazioni:
   - il nome ed i dati di contatto dell'Università e del DPO;
   - le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
   - i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 del Regolamento UE, la documentazione delle garanzie adeguate;
   - la descrizione generale delle misure di sicurezza tecniche ed organizzative del trattamento adottate sulla base del contratto o atto giuridico che definisce la nomina, da parte del titolare, a responsabile del trattamento.

Articolo 21 - Sensibilizzazione e formazione

1. Ai fini della corretta e puntuale applicazione della disciplina in materia di protezione dei dati personali e della sicurezza informatica, l'Università sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo l'Università promuove l'attività formativa del personale universitario e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Università.
2. L'Università predispone ogni anno, sentito il 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. Tale formazione, sentito il RPCT, è integrata e coordinata con la formazione in materia di prevenzione della corruzione, nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'Università.
3. La frequenza delle attività di formazione in materia di privacy è obbligatoria, ai sensi degli artt. 29, 32, paragrafo 4, e 39, paragrafo 1, lettera b), del Regolamento UE.

Articolo 22 - Valutazione d'impatto sulla protezione dei dati (DPIA)

1. Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il designato o suo referente, previa consultazione con il DPO, effettua, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali.
2. L'ufficio dell'Amministrazione competente in materia di protezione dei dati personali offre il necessario supporto alla redazione della valutazione di impatto.

3. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.
4. La valutazione d'impatto sulla protezione dei dati è obbligatoria nei casi seguenti:
   a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
   b. il trattamento, su larga scala, di categorie particolari di dati personali quali: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati;
   c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza) e/o con l'utilizzo con sistemi intelligenti;
   d. il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.
5. Il designato o suo referente consulta il DPO anche per assumere la decisione di effettuare o meno la valutazione di impatto. Tale consultazione e le conseguenti decisioni assunte dal designato o suo referente devono essere documentate nell'ambito della valutazione di impatto. Il designato o suo referente è tenuto a documentare le motivazioni nel caso adotti condotte difformi da quelle raccomandate dal DPO.
6. Il responsabile per la sicurezza e per la transizione al digitale fornisce supporto ai designati o loro referenti e al DPO per lo svolgimento della valutazione di impatto.
7. L'Università, tramite il 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 e che le misure tecniche e organizzative individuate non sono sufficienti a mitigare adeguatamente i rischi per i diritti e le libertà degli interessati.
8. 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, ai sensi dell'art. 110 del Codice in materia di protezione dei dati personali, il titolare del trattamento deve adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati. Questo include ottenere il parere favorevole del comitato etico competente e condurre una valutazione di impatto sulla protezione dei dati (DPIA).

Articolo 23 - Misure tecniche e organizzative

1. L'Università mette in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato per i diritti e le libertà delle persone fisiche, in relazione ai probabili rischi derivanti dal trattamento dei dati personali.
2. Nel valutare l'adeguato livello di sicurezza, l'Università tiene conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non

autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'Università effettua la valutazione dei rischi connessi al trattamento e adotta misure di sicurezza comprendenti, tra le altre:
   - la pseudonimizzazione e la cifratura dei dati;
   - le misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni;
   - la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico;
   - procedure atte a verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
4. Le misure tecniche sono riesaminate in modo periodico dall'Area Sistemi Informativi e Portale di Ateneo, sentito il responsabile della protezione dati (DPO) e l'ufficio dell'Amministrazione competente in materia di protezione dei dati personali. Le suddette misure sono pubblicate sulla rete intranet e sono illustrate nelle sessioni formative.
5. L'Università considera rischioso il trasporto di dati personali su supporto fisico (computer portatili, copie cartacee, pendrive ecc.). Ciò vale prioritariamente per le categorie particolari di dati, i grandi volumi di dati personali e le informazioni che comportano particolari rischi per l'interessato nel caso di perdita o distruzione. Solo in circostanze eccezionali tali dati possono essere trasportati fuori dagli ambienti dell'Università e sotto la diretta responsabilità di personale autorizzato. In particolare, il personale autorizzato è tenuto a:
   - ove possibile fare uso di accesso remoto tramite *login* e *password* alle informazioni;
   - trasportare solo la quantità minima di dati personali;
   - assicurarsi che i dispositivi mobili e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali fuori dagli ambienti universitari siano dotati di sistemi di crittografia.
6. Qualunque perdita e/o furto di dati deve essere tempestivamente segnalato e trattato secondo la procedura di gestione delle violazioni di dati personali di cui al successivo art. 25.
7. I designati, gli autorizzati e i referenti sono tenuti a custodire e trattare i dati applicando le misure idonee ad evitare rischi di distruzione o perdita, anche accidentale, e di accesso non autorizzato, definite dalla specifica *policy* di Ateneo o riportate nell'atto di nomina.
8. Tutti i designati sono tenuti ad adottare le misure di sicurezza, ulteriori rispetto a quelle minime prescritte dalla normativa nazionale a tutela della riservatezza dei dati personali, che si rendano necessarie in relazione a specifiche esigenze della struttura gestita, tenuto conto del livello di esposizione a rischio cui sono soggette le attività di trattamento dei dati affidate, della peculiarità e delicatezza dei trattamenti effettuati, nonché dello sviluppo tecnologico.
9. Ai designati è richiesto di vigilare sul rispetto, da parte degli autorizzati/referenti, delle misure di sicurezza.
10. Tutti i sistemi di intelligenza artificiale utilizzati dall'amministrazione devono essere trasparenti e spiegabili. Gli utenti devono essere informati quando interagiscono con un sistema di IA e devono avere accesso a spiegazioni comprensibili delle decisioni assunte

in forma automatizzata. Prima dell'implementazione di qualsiasi sistema di IA, deve essere condotta una valutazione del rischio per identificare e mitigare potenziali impatti negativi sui diritti e le libertà fondamentali degli interessati.

11. L'amministrazione deve istituire un piano di gestione degli incidenti che includa procedure per la rilevazione, la risposta e la notifica degli incidenti di sicurezza informatica, in conformità con la direttiva NIS.2 (*Network and Information Security*).
12. Per quanto non espressamente disciplinato dal presente articolo, si rinvia al regolamento di Ateneo sull'utilizzo della rete internet e dei servizi informatici e alle relative Linee guida dei servizi in rete, nonché alle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte dall' Agenzia per l'Italia Digitale (AgID).

Articolo 24 - Uso della Virtual Desktop Infrastructure (VDI) e misure di sicurezza

1. L'Università può adottare sistemi di *Virtual Desktop Infrastructure* (VDI) per garantire al personale di Ateneo un accesso remoto, sicuro, controllato e conforme alla normativa vigente, alle risorse informatiche di Ateneo e ai dati personali trattati nell'ambito delle proprie attività istituzionali.
2. L'adozione e l'utilizzo della VDI devono essere disciplinati da adeguate linee guida, approvate dal Consiglio di Amministrazione, che definiscano le modalità d'uso, le responsabilità degli utenti e le misure di sicurezza applicabili.
3. Prima dell'attivazione del sistema o di modifiche sostanziali alla sua configurazione, devono essere predisposti:
   - una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 del Regolamento UE;
   - una specifica informativa agli interessati, redatta in conformità agli artt. 12-14 del Regolamento UE.
4. Devono essere adottate misure tecniche e organizzative idonee a garantire la tutela delle prerogative individuali e sindacali dei lavoratori, in conformità alla normativa italiana vigente, con particolare riferimento allo Statuto dei lavoratori.
5. Il sistema VDI deve garantire, in particolare:
   - l'accesso esclusivamente previa autenticazione forte, mediante credenziali personali, non cedibili;
   - la cifratura dei dati in transito e a riposo;
   - la segmentazione delle sessioni utente, per prevenire accessi non autorizzati;
   - l'utilizzo esclusivo per finalità lavorative istituzionali;
   - la registrazione e il monitoraggio degli accessi e delle attività degli amministratori di sistema, con produzione di report periodici;
   - la disconnessione automatica delle sessioni in caso di inattività prolungata.
6. Il personale autorizzato all'uso della VDI deve essere preventivamente informato e formato sull'utilizzo del sistema e sulle misure di sicurezza applicabili.
7. Il responsabile della protezione dei dati deve essere coinvolto preventivamente in ogni fase di progettazione, attivazione o modifica sostanziale dell'infrastruttura VDI, nonché in caso di introduzione di nuove funzionalità che comportino trattamenti di dati personali.

Articolo 25 - Violazione dei dati personali (data breach)

1. Si intende per violazione dei dati personali una violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
2. Al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati, l'Università in qualità di titolare del trattamento definisce una procedura di gestione delle violazioni di dati personali.
3. Tale procedura si applica a qualunque attività svolta dall'Università con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.
4. La procedura definisce le modalità per identificare la violazione, analizzare le cause della violazione, definire le misure da adottare per rimediare alla violazione dei dati personali, attenuarne i possibili effetti negativi, registrare le informazioni relative alla violazione, identificare le azioni correttive e valutarne l'efficacia, notificare la violazione di dati personali al Garante nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche, comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio sia elevato.
5. La procedura è resa disponibile attraverso la rete intranet di Ateneo.
6. L'Università pianifica sezioni di informazioni e formazione finalizzate ad illustrare la procedura del *data breach*, in termini di ruoli, compiti, responsabilità e sanzioni.
7. Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa può comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

Articolo 26 - Sanzioni

1. L'illecito trattamento dei dati personali determina in capo ai trasgressori le seguenti forme di responsabilità:
   a. penale, per le violazioni di cui agli artt. 167, 167-bis, 167-ter e 168 del Codice in materia di protezione dei dati personali;
   b. civile, per i danni materiali e immateriali causati agli interessati, ai sensi dell'art. 82 del medesimo Regolamento UE;
   c. amministrativa, con l'applicazione delle sanzioni pecuniarie di cui all'art. 83 del Regolamento UE.
2. Ai sensi dell'art. 2-*decies* del d.lgs. 196/2003, i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall'art. 160-*bis* per i procedimenti giudiziari.
3. 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.

TITOLO V
DIRITTI DEGLI INTERESSATI

Articolo 27 - Diritti dell'interessato

1. L'Università garantisce il rispetto dei diritti degli interessati previsti dagli artt. 12-22 del Regolamento UE. In particolare, l'interessato può:
   a. ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
   b. ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento;
   c. esercitare il diritto alla limitazione del trattamento non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, o dell'accertamento dei diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante;
   d. esercitare il diritto di opposizione alla profilazione;
   e. esercitare il diritto alla portabilità dei dati solo qualora il trattamento si basi sul consenso ai sensi dell'art. 6. par. 1, lettera a), o dell'art. 9, par. 2, lettera a) del Regolamento UE o su un contratto ai sensi dell'art. 6, par. 1, lettera b) del Regolamento UE e sia effettuato con mezzi automatizzati. Tale diritto non si applica al trattamento necessario per l'esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Università;
   f. esercitare il diritto all'oblio chiedendo la cancellazione dei propri dati personali nel caso questi siano stati resi pubblici on-line. Tale diritto può essere esercitato ove ricorra una delle seguenti fattispecie:
      - i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
      - l'interessato revoca il consenso su cui si basa il trattamento;
      - l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
      - i dati personali sono trattati illecitamente;
      - adempimento di un obbligo legale;
      - i dati riguardino minori.
2. L'Università informa della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione.
3. L'interessato può esercitare i suoi diritti con richiesta scritta indirizzata al responsabile della struttura competente per la gestione dei dati personali oggetto della richiesta e in alternativa al designato o suo referente.
4. Il riscontro alla richiesta presentata dall'interessato viene fornito dal responsabile della struttura che tratta i dati, 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 30 giorni dall' acquisizione della richiesta al protocollo.

5. Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.
6. L'Università, tramite i designati o loro referenti, agevola l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa.
7. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.
8. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, l'Università può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi sostenuti oppure può rifiutare di soddisfare la richiesta, dimostrando il carattere manifestamente infondato o eccessivo della richiesta. Il Consiglio di Amministrazione stabilisce i criteri per la definizione delle modalità di pagamento e dell'importo del contributo spese da parte degli interessati.
9. La modulistica per l'esercizio dei sopra citati diritti è redatta e aggiornata a cura dei designati o loro referenti che devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi, nei casi più complessi, del supporto del DPO.
10. Le richieste di esercizio di diritti da parte degli interessati sono inserite all'interno di un registro entro 30 giorni dalla data di conclusione del procedimento.
11. Nei casi di trattamenti di dati esternalizzati, il responsabile del trattamento è tenuto a collaborare con l'Università.

Articolo 28 - Informazioni agli interessati

1. Per ogni tipologia di trattamento dei dati l'Università, salvo il caso in cui l'interessato sia già in possesso delle informazioni, fornisce l'informativa all'interessato, di cui all'art. 13, o nei casi previsti, all'art. 14 del Regolamento UE. L'informativa 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 del presente regolamento;
   - gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
   - l'eventuale volontà dell'Università di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di un fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
   - il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;

- i diritti che l'interessato può esercitare, quali: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione, il diritto alla portabilità dei dati, la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, il diritto di proporre reclamo al Garante per la protezione dei dati personali;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.

3. Nel caso in cui i dati personali debbano essere trattati per una finalità diversa da quella per cui sono stati raccolti, l'Università fornisce all'interessato informazioni in merito alla diversa finalità prima di tale ulteriore trattamento.
4. Nel caso in cui i dati non siano raccolti presso l'interessato, l'Università si riserva la possibilità di non fornire l'informativa nel caso in cui l'interessato già disponga delle informazioni oppure comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.
5. Le informative di competenza delle strutture sono aggiornate dai designati o loro referenti.
6. 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.
7. Il personale e chiunque operi sotto l'autorità dell'Università può trattare i dati personali solo per le specifiche finalità indicate nell'informativa fornita all'interessato al momento del conferimento dei dati o per ogni altra finalità prevista dalla legge. I dati personali non possono essere usati per finalità diverse da quelle per le quali sono stati raccolti. Se si rendesse necessario modificare le finalità del trattamento, l'interessato dovrà essere informato della nuova finalità prima dell'inizio di qualunque trattamento. Fanno eccezione a questa disposizione i trattamenti effettuati per finalità di ricerca.

Articolo 29 - Accesso ai documenti amministrativi e accesso civico

1. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e per l'esercizio dell'accesso civico restano disciplinati dalla legge 7 agosto 1990, n. 241 e successive modificazioni, dal decreto legislativo 14 marzo 2013, n. 33 e successive modificazioni, dagli articoli 59 e 60 del Codice in materia di protezione dei dati personali e successive modificazioni, nonché dai regolamenti di Ateneo.

2. L'Ateneo assicura che l'accesso avvenga nel rispetto dei principi di cui al Regolamento UE, in particolare minimizzazione, proporzionalità e sicurezza, e che siano adottate misure idonee a tutelare i diritti e le libertà degli interessati.
3. In caso di documenti contenenti categorie particolari di dati personali o dati giudiziari, l'accesso è consentito solo se strettamente necessario per la tutela di interessi giuridicamente rilevanti e nel rispetto delle garanzie previste dalla normativa vigente.
4. L'Ateneo garantisce la comunicazione ai controinteressati e il rispetto delle esclusioni e limitazioni previste dalla legge e dai regolamenti interni, in particolare per motivi di sicurezza, segreto d'ufficio, riservatezza di terzi e tutela di dati sensibili.
5. L'Ateneo si conforma alle linee guida dell'Autorità Nazionale Anticorruzione (ANAC) e del Garante per la protezione dei dati personali in materia di accesso civico, trasparenza e protezione dei dati.

TITOLO VI
COMUNICAZIONE E DIFFUSIONE DEI DATI

Articolo 30 - Circolazione dei dati all'interno dell'Ateneo

1. L'accesso e l'utilizzo dei dati all'interno delle strutture e da parte dei dipendenti dell'Università, in ragione delle specifiche funzioni assegnate, è ispirato al principio della libera circolazione delle informazioni finalizzate 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. Le informazioni devono essere rese disponibili esclusivamente ai soggetti, strutture e dipendenti dell'Università, che hanno necessità di accedervi per lo svolgimento dell'attività inerente alla loro specifica funzione. 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 31 - Comunicazione e diffusione di dati personali

1. La comunicazione e la diffusione dei dati personali, esclusi i dati di cui all'art. 13, sono permesse quando:
   a. siano previste da norme di legge, di regolamento o dal diritto dell'Unione europea;
   b. siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o aggregati;
   c. siano richieste per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia;

d. siano necessarie per il soddisfacimento di richieste di accesso ai sensi dell'art. 29.

2. La comunicazione di dati a soggetti pubblici è sempre ammessa per i fini istituzionali e ove prevista da norma di legge o di regolamento o da atti amministrativi generali, secondo quanto previsto dall'art. 2-*ter* del Codice in materia di protezione dei dati personali.
3. Le richieste da parte di soggetti privati ed enti pubblici economici volte ad ottenere la comunicazione di dati, devono essere formulate per iscritto e motivate e devono contenere: il nome, la denominazione o la ragione sociale del richiedente; l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.
4. L'Università, nella figura del designato o suo referente, valuta, sulla base di quanto disposto dalle norme vigenti in materia di protezione dei dati personali e di quanto previsto dal presente regolamento, eventuali richieste di comunicazione di dati personali a soggetti privati e decide in ordine all'opportunità di effettuare la comunicazione.
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 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.
8. 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. 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.
9. In considerazione del sistema di autovalutazione, accreditamento e valutazione periodica dei Corsi di studio definito dal MUR, 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 disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti per i quali non è prevista la pubblicazione obbligatoria, procedendo all'indicazione in forma anonima dei dati personali eventualmente presenti, ai sensi dell'art. 7-*bis*, comma 3, del d.lgs. 14 marzo 2013, n. 33.
11. Quando norme di legge o di regolamento impongono la pubblicazione di specifici atti o documenti, contenenti dati personali, l'Università provvede a rendere non intelligibili i dati personali che non siano pertinenti o necessari rispetto alla specifica finalità di

trasparenza che la pubblicazione intende perseguire, ai sensi dell'art. 7-*bis*, comma 4, del d.lgs. 33/2013.

12. Se gli atti o i documenti da pubblicare, di cui al precedente comma, contengono dati sensibili o dati giudiziari, l'Università ha l'obbligo di renderli non intelligibili, a meno che tali dati non siano indispensabili per le già menzionate finalità di trasparenza.
13. In ogni caso, è vietata la diffusione di dati genetici e biometrici e di dati idonei a rivelare lo stato di salute e la vita sessuale dell'interessato, ai sensi dell'art. 2-*septies*, comma 8, del Codice in materia di protezione dei dati personali e dell'art. 7-*bis*, comma 6, del d.lgs. 33/2013.
14. I responsabili delle strutture di Ateneo che propongono delibere, che adottano decreti o altri provvedimenti, destinati alla pubblicazione, verificano, nel rispetto del principio di minimizzazione dei dati di cui all'art. 5 del Regolamento UE, che l'inclusione nel testo di dati personali sia realmente necessaria per perseguire le finalità specifiche del provvedimento. Devono essere privilegiate modalità di redazione che prevedano l'utilizzo di dati anonimi o non direttamente identificativi, quali codici o altri riferimenti, se lo scopo cui l'atto è preordinato è ugualmente raggiungibile.
15. Laddove gli allegati alle delibere o ai decreti/provvedimenti contengano dati sensibili, che non è possibile rendere anonimi, nel provvedimento deve essere evidenziato che l'allegato non può essere pubblicato, rimanendo depositato agli atti presso la struttura organizzativa, per esigenze di tutela della riservatezza dei destinatari del provvedimento o di terzi. Sull'allegato deve essere apposta la dizione "Riservato ai sensi delle vigenti norme sulla privacy".
16. Con riferimento ai dati contenuti nei provvedimenti/atti da pubblicare, dovranno essere rispettate le seguenti indicazioni di massima:
    - ove possibile e salvo diversa disposizione contraria, verrà inserito il solo nome e cognome dell'interessato richiamato nell'atto amministrativo; la data di nascita verrà indicata solo in caso di omonimia e in nessun caso verrà riferito il codice fiscale.
    - nei provvedimenti in cui vi è anche indirettamente la possibilità di rivelare informazioni sullo stato di salute, l'origine nazionale e/o altre categorie particolari di dati, è necessario oscurare il nome e il cognome dell'interessato o indicarne le sole iniziali.
    - nei documenti analogici digitalizzati è necessario oscurare la firma autografa del soggetto che ha sottoscritto il documento.

Articolo 32 - 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, ai sensi dell'art. 100 del Codice in materia di protezione dei dati personali, comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei trattamenti di categorie particolari di dati personali e dei trattamenti di dati personali relativi a condanne penali e reati.
2. 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.

3. 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 33 - 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 sul Portale di Ateneo i bandi di concorso per il reclutamento, a qualsiasi titolo, di personale presso l'Amministrazione, nonché i criteri di valutazione delle Commissioni, le tracce delle prove, le graduatorie finali con i soli partecipanti risultati vincitori, l'eventuale scorrimento degli idonei non vincitori.
2. Le ulteriori informazioni relative ai concorsi, compresi il diario delle prove e il loro esito, sono rese disponibili agli aventi diritto tramite l'accesso ad aree riservate del Portale di Ateneo, consultabili da remoto con credenziali di autenticazione.
3. La pubblicazione dei dati sul Portale di Ateneo è effettuata, in ogni caso, nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati e secondo le indicazioni fornite dal Garante per la protezione dei dati personali. In particolare, per pubblicare le graduatorie dei concorsi pubblici rispettando la normativa sulla trasparenza e la protezione dei dati personali, senza eccedere in dettagli che possano compromettere la riservatezza dei partecipanti, è necessario seguire le seguenti linee guida:
   - pubblicare i bandi di concorso, i criteri di valutazione, le tracce delle prove scritte e le graduatorie finali aggiornate con l'eventuale scorrimento degli idonei non vincitori.
   - le graduatorie devono essere pubblicate tempestivamente e aggiornate costantemente.
   - le graduatorie finali devono riportare solo il nome e il cognome del vincitore o dei vincitori, evitando ulteriori dati personali (come, ad esempio, la data di nascita).
   - non è consentito pubblicare l'elenco dei partecipanti non ammessi o esclusi.
   - i risultati delle prove scritte e orali non devono essere pubblicati, ma possono essere comunicati direttamente ai candidati o resi noti solo nell'ambito di un esercizio del diritto di accesso agli atti da parte di eventuali controinteressati.

- è consentito pubblicare, nelle graduatorie finali, esclusivamente i nomi dei vincitori, anche se altri candidati sono risultati idonei, e le determinazioni di scorrimento dei candidati idonei non vincitori indicando esclusivamente il nome del candidato successivamente assunto.
- è vietata la pubblicazione di elenchi nominativi dei partecipanti ammessi alle prove scritte o orali.

TITOLO VII
DISPOSIZIONI FINALI

Articolo 34 - Norme di rinvio

1. Per tutto quanto non disciplinato dal presente Regolamento si fa rinvio a:
   - Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
   - Decreto Legislativo 196/2003 recante "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni;
   - Decreto Legislativo 101/2018 (Decreto di armonizzazione della normativa nazionale al Regolamento UE 2016/679);
   - Legge 7 agosto 1990, n. 241, recante “Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”, come successivamente modificata;
   - D.lgs. 14 marzo 2013, n. 33 “Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni” e sue modifiche e integrazioni;
   - Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (NIS.2);
   - art. 391-*quater* del Codice di procedura penale;
   - provvedimento generale del Garante per la protezione dei dati personali in materia di videosorveglianza dell’8 aprile 2010 e normativa ivi richiamata;
   - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati;
   - Linee guida e di indirizzo e regole deontologiche adottate e approvate dal Garante per la protezione dei dati personali;
   - Legge 20 maggio 1970, n. 300, recante lo Statuto dei lavoratori, con particolare riferimento all’art. 4;
   - Regolamento (UE) 2024/1689 del 13 giugno 2024 sull’intelligenza artificiale e conseguente normativa nazionale;
   - Vigente Regolamento dell’Università in materia di videosorveglianza.

Articolo 35 - Disposizioni finali ed efficacia

1. Il presente regolamento, acquisito il parere del Senato Accademico è approvato dal Consiglio di Amministrazione ed emanato con Decreto Rettorale.
2. Il presente regolamento modifica e sostituisce il regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio nonché del Decreto legislativo 30 giugno 2003, n. 196 codice in materia di protezione dei dati personali, emanato con D.R. n. 401 del 18 novembre 2019.
3. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento (UE) 2016/679 e del d.lgs. 196/2013 Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dall'Autorità Garante.
4. Al fine di attuare le azioni previste, il CdA valuta per le strutture decentrate la necessità di integrare la pianta organica con personale tecnico amministrativo dedicato e individua, di concerto con la Direzione Generale, le opportune e specifiche attività di formazione del personale.
5. Per le materie disciplinate dal presente regolamento che richiedano un'applicazione più dettagliata o specifica, il Consiglio di Amministrazione provvede, ove necessario, all'adozione di apposite linee guida.
6. Il presente regolamento entra in vigore il giorno successivo alla data della sua emanazione.
7. L'Università provvede a dare pubblicità al presente regolamento e alle successive modifiche ed integrazioni mediante pubblicazione sul sito *web* d'Ateneo.

Firmato digitalmente da: Massimo Midiri
Organizzazione: UNIVERSITA' DEGLI STUDI DI PALERMO/80023730825
Data: 16/03/2026 15:40:36