UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
UFFICIO SEGRETERIA DEL DIRETTORE GENERALE
DR/2026/111 del 15/01/2026
Firmatari: LORITO Matteo

U.S.R.

IL RETTORE

VISTO il vigente Statuto dell'Ateneo;
VISTO il Regolamento generale dell'Unione Europea sulla protezione dei dati (GDPR) n. 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, che abroga la sopra citata Direttiva Europea n. 95/46/CE (Regolamento generale sulla protezione dei dati);
VISTO il D.Lgs. n. 101 del 10 agosto 2018, - recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del suddetto Regolamento (UE) 2016/679 – con il quale sono state apportate modifiche al *Codice in materia di protezione dei dati personali* di cui al D.Lgs. 30 giugno 2003, n. 196;
VISTE le Linee Guida in materia di trattamento di dati personali, emanate dal Comitato europeo per la protezione dei dati Personali e dall'Autorità Garante per la protezione dei dati personali nonché le Linee Guida in materia di sicurezza ICT per le Pubbliche Amministrazioni, emanate dall'Agenzia per l'Italia Digitale (AgID) e finalizzate, tra l'altro, alla protezione dei dati personali trattati con strumenti informatici;
VISTO il D.lgs. 14 marzo 2013, n. 33 e ss.mm.ii., in tema di riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
VISTO il *Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei dati personali*, emanato con D.R. n. 1226 del 19/03/2021;
RITENUTO opportuno revisionare il sopra citato *Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei Dati Personali*, al fine di strutturarne il testo e i contenuti in maniera più organica e completa, apportando allo stesso le modifiche/integrazioni, di seguito sinteticamente descritte:

- integrazione del richiamo ai principi generali applicabili al trattamento dei dati personali tra i quali i pincipi della *accountability*, della *privacy by design* e della *privacy by default*;
- integrazione della declaratoria delle condizioni di liceità del trattamento (c.d. basi giuridiche), in presenza delle quali il trattamento dei dati personali effettuato dall'Università e dalle sue diverse articolazioni può definirsi lecito;
- introduzione della previsione degli adempimenti che l'Ateneo, in qualità di titolare del trattamento, in virtù della normativa applicabile, è tenuto a porre in essere;
- ridefinizione dei soggetti a vario titolo coinvolti nel trattamento dei dati personali presso questo Ateneo e delle rispettive funzioni e responsabilità;
- revisione delle disposizioni riguardanti l'informativa privacy ed il trattamento di dati personali in particolari contesti, quali: il rapporto di lavoro, l'archiviazione, la ricerca scientifica, gli organi collegiali, ecc.;

VISTA la Delibera n. 30 del 26/11/2025 (EO n. 1471 del 03/12/2025) con la quale il Senato Accademico, subordinatamente al parere favorevole del Consiglio di Amministrazione, ha approvato la nuova stesura del *Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei Dati Personali,* recante le sopra cennate modifiche/integrazioni;
VISTA la Delibera n. 85 del 26/11/2025 (EO n.1512 del 05/12/2025) con la quale il Consiglio di Amministrazione ha espresso parere favorevole in merito alla nuova stesura del sopra citato *Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei Dati Personali*, recante le sopra cennate modifiche/integrazioni;

DECRETA

È emanato - nel testo allegato al presente Decreto di cui costituisce parte integrante e sostanziale - il *Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei Dati Personali*, recante le modifiche accennate in premessa.

Il sopra citato Regolamento entra in vigore il giorno successivo alla sua pubblicazione all'Albo Ufficiale di questa Università e, da quella data, sostituisce il Regolamento emanato con il sopra citato D.R. n. 1226/2021.

Area Affari Generali e Gestione Documentale
Il Dirigente: *dott. Francesco BELLO*
Unità organizzativa responsabile del procedimento:
Ufficio Statuto, Regolamenti e Organi Universitari
Responsabile del Procedimento:
Il Capo dell'Ufficio: *dott. Antonio NASTI*

IL RETTORE
Matteo LORITO

Regolamento in materia di trattamento dei dati personali dell'Università degli Studi di Napoli Federico II

TITOLO I
PRINCIPI E DISPOSIZIONI GENERALI

CAPO I
OGGETTO, AMBITO DI APPLICAZIONE E DEFINIZIONI

Articolo 1
Oggetto

Il presente Regolamento, adottato in attuazione del Regolamento (UE) 2016/679 e del Decreto Legislativo n. 196/2003 come novellato dal Decreto Legislativo n. 101/2018 e ss.mm.ii., disciplina la tutela delle persone fisiche con riguardo al trattamento dei dati personali all'interno dell'Università degli Studi di Napoli Federico II.

Articolo 2
Ambito di applicazione

Il presente Regolamento si applica al trattamento dei dati personali che l'Università effettua per il perseguimento dei propri fini istituzionali, nei limiti stabiliti dallo Statuto, dalle leggi e dai regolamenti e, in ogni caso, nel rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato.

Articolo 3
Definizioni

3.1 Ai fini del presente Regolamento, s'intende per:

1. "**Università**": l'Università degli Studi di Napoli Federico II;
2. "**Regolamento UE**": il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; il Regolamento (UE) 2016/679 abroga la Direttiva 95/46/CE;
3. "**Codice Privacy**": il Decreto Legislativo 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", così come modificato e integrato dal Decreto Legislativo 10 agosto 2018 n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", e ss.mm.ii.;
4. "**Regolamento**": il Regolamento dell'Università degli Studi di Napoli Federico II in materia di trattamento dei dati personali;
5. "**Dato Personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
6. "**Interessato**": la persona fisica, identificata o identificabile, cui si riferiscono i dati personali;

7. “**Categorie Particolari di Dati Personali**”: i dati personali che rivelino 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;
8. “**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;
9. “**Dati Genetici**”: i dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall’analisi di un campione biologico della persona fisica in questione;
10. “**Dati Biometrici**”: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano o confermino l’identificazione univoca, quali, ad esempio, i dati dattiloscopici;
11. “**Dati relativi alla salute**”: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute;
12. “**Dati Personali Giudiziari**”: i dati personali relativi a condanne penali e reati o a connesse misure di sicurezza;
13. “**Trattamento**”: qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione;
14. “**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;
15. “**Pseudonimizzazione**”: il trattamento dei dati personali in modo tale che gli stessi 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;
16. “**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;
17. “**Contitolare del Trattamento**”: 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;
18. “**Responsabile per la Protezione dei Dati**” o “**Data Protection Officer**” (“RPD” o “DPO”): figura indipendente che svolge attività di consulenza, supporto e controllo per il corretto adeguamento dell’Università al Regolamento UE nonché di raccordo tra il Titolare del Trattamento e l’Autorità Garante per la Protezione dei Dati Personali;
19. “**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;

20. "**Sub-Responsabile del Trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo a cui il responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
21. "**Struttura**": le Aree dell'Amministrazione Centrale e i relativi Uffici, i Dipartimenti e i relativi Uffici, le Scuole e i relativi Uffici, i Centri dell'Ateneo, le Biblioteche di Area, i Musei, l'Orto Botanico, l'Azienda Agraria e Zootecnica;
22. "**Organi**" "**Comitati**" "**Commissioni**": Organi, Comitati, Commissioni e altri Organismi a vario titolo istituiti nell'ambito dell'Università;
23. "**Responsabile Privacy**": il soggetto che, in ragione della carica istituzionale ricoperta, è individuato tale ai sensi dell'articolo 9, comma 1, del presente Regolamento;
24. "**Referente**": il soggetto che, in ragione della funzione organizzativa ricoperta, è individuato tale ai sensi dell'articolo 11 del presente Regolamento;
25. "**Autorizzato al Trattamento**": chiunque agisca sotto l'autorità diretta dell'Università che abbia accesso ai dati personali; non può trattare tali dati se non è istruito in tale senso dal Titolare del Trattamento;
26. "**Autorità Garante**": Autorità Garante per la Protezione dei Dati Personali. L'autorità pubblica indipendente italiana istituita ai sensi dell'articolo 51 del Regolamento UE;
27. "**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;
28. "**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 e gli Autorizzati al trattamento dei dati personali sotto l'autorità diretta del Titolare del Trattamento o del Responsabile del Trattamento;
29. "**Destinatario**": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione 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;
30. "**Violazione dei dati personali**": l'evento 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;
31. "**Comunicazione**": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare del Trattamento nel territorio dell'Unione europea, dal Responsabile del Trattamento o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate ai sensi dell'articolo 2-*quaterdecies* del Codice Privacy, al trattamento dei dati personali sotto l'autorità diretta del Titolare del Trattamento o del Responsabile del Trattamento, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
32. "**Diffusione**": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

3.2 Per tutte le definizioni non espressamente riportate nel presente articolo, si rinvia all'articolo 4 del Regolamento UE.

CAPO II
PRINCIPI GENERALI

Articolo 4
Principi generali applicabili al trattamento dei dati personali

L'Università tratta i dati personali nel rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati. In particolare, ai sensi e per gli effetti dell'articolo 5 del Regolamento UE, i dati personali oggetto di trattamento da parte dell'Università sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principio di liceità, correttezza e trasparenza);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, del Regolamento UE, considerato incompatibile con le finalità iniziali (principio di limitazione della finalità);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di 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, conformemente all'articolo 89, paragrafo 1, del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (principio di limitazione della conservazione);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di integrità e riservatezza).

Articolo 5
Principio di responsabilizzazione (c.d. "accountability")

L'Università, in ogni sua articolazione, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate ed efficaci per garantire ed essere in grado di dimostrare la conformità dei trattamenti di dati personali alle prescrizioni del Regolamento UE.

Articolo 6
Principi di *privacy by design* e *privacy by default*

6.1 L'Università, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso, mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento UE e tutelare i diritti degli interessati ("principio di *privacy by design*" o di "protezione dei dati fin dalla progettazione").

6.2 L'Università mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica ("principio di *privacy by default*" o "principio di protezione dei dati per impostazione predefinita").

6.3 In ragione di quanto disposto dal presente articolo, ciascuna Struttura, Organo, Comitato, Commissione e altro Organismo dell'Università è tenuta a individuare e implementare le predette misure tecniche e organizzative, nonché a vigilare sul rispetto delle stesse.

Articolo 7
Condizioni di liceità del trattamento

7.1 L'Università può trattare dati personali esclusivamente in presenza di almeno una delle condizioni di liceità (o c.d. "base giuridica") tra quelle di seguito elencate:

a) esecuzione dei compiti di interesse pubblico e connessi all'esercizio di pubblici poteri attribuiti all'Università da norme di legge o di regolamento;
b) esecuzione di un contratto di cui l'interessato è parte o esecuzione di misure precontrattuali adottate su richiesta dell'interessato stesso;
c) adempimento di obblighi di legge a cui è soggetta l'Università;
d) salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
e) consenso dell'interessato, ove consentito, anche in considerazione dei pareri e dei provvedimenti dell'Autorità Garante;
f) al di fuori dei propri compiti istituzionali, nel perseguimento del legittimo interesse dell'Università o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

7.2 Qualora il trattamento sia basato sul consenso, l'Università informa previamente l'interessato e acquisisce il consenso con modalità atte a dimostrare che l'interessato ha prestato il proprio consenso espresso, libero, consapevole, inequivocabile, al trattamento dei propri dati personali. 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.

7.3 In applicazione dei principi di cui al Regolamento UE, ciascuna Struttura dell'Università, nell'esercizio delle sue funzioni, individua la/le corretta/e condizione di liceità, tra quelle elencate al precedente comma 1, per le attività di trattamento poste in essere, confrontandosi, se del caso, con l'RPD dell'Università.

TITOLO II
ADEMPIMENTI NELL'AMBITO DEL TRATTAMENTO DEI DATI PERSONALI

CAPO III
SOGGETTI DEL TRATTAMENTO E RESPONSABILITÀ

Articolo 8
Titolare del trattamento

8.1 Il titolare del trattamento è l'Università degli Studi di Napoli Federico II nel suo complesso, il cui rappresentante legale è il Magnifico Rettore *pro tempore*.

8.2 L'Università adotta misure tecniche e organizzative adeguate al fine di garantire ed essere in grado di dimostrare la conformità del trattamento al Regolamento UE e al Codice Privacy, tenendo conto della natura, dell'ambito di applicazione, del contesto, della condizione di liceità e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure sono periodicamente riesaminate e aggiornate. Nello specifico, l'Università, in qualità di titolare del trattamento, deve, tra l'altro:

a. disciplinare con un contratto o altro atto giuridico i trattamenti posti in essere da ciascun Responsabile del trattamento, come specificato al successivo articolo 14 del presente Regolamento;
b. fornire le informazioni sul trattamento dei dati personali agli interessati di cui al successivo articolo 17;
c. definire gli adempimenti finalizzati alla tutela della sicurezza dei dati personali oggetto del trattamento;
d. tenere il registro delle attività di trattamento di cui al successivo articolo 18;
e. dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al successivo articolo 20;
f. effettuare la valutazione di impatto sulla protezione dei dati e notificare all'Autorità Garante, se del caso, le violazioni di dati personali;
g. valutare, in base alle condizioni di cui al successivo articolo 35, comma 4, la necessità di comunicare all'interessato le violazioni di dati personali di cui al punto precedente;
h. designare il Responsabile della Protezione dei Dati di cui al successivo articolo 15.

Articolo 9
Responsabili Privacy

9.1 Fatto salvo quanto previsto al precedente articolo 8, comma 1, tenuto conto dell'attuale assetto organizzativo dell'Università, con il presente Regolamento si individuano quali Responsabili Privacy, in ragione della funzione apicale ricoperta, dei compiti e delle relative responsabilità, i seguenti soggetti:

a. il Direttore Generale;
b. i Presidenti delle Scuole;
c. i Direttori di Dipartimento;
d. i Presidenti/Direttori dei Centri di Ricerca, Centri di Servizio Interdipartimentali e Centri di Servizio dell'Ateneo;
e. i Direttori dei Musei;
f. il Direttore dell'Orto Botanico;
g. il Presidente dell'Azienda Agraria e Zootecnica;
h. i Dirigenti delle Aree;
i. i Direttori delle Scuole di Specializzazione.

9.2 I soggetti individuati al precedente comma 1 devono garantire, all'interno delle proprie Strutture e delle rispettive diramazioni/strutture afferenti, il rispetto delle norme vigenti in materia di protezione dei dati personali e del presente Regolamento. In particolare, congiuntamente e con il supporto dei Referenti, come individuati al successivo articolo 11, i Responsabili Privacy hanno il compito di:

1. conoscere e rispettare le disposizioni del Regolamento UE, del Codice Privacy, del presente Regolamento, le istruzioni impartite dal Titolare del Trattamento in materia di protezione dei dati personali attraverso il Disciplinare attualmente vigente ed i loro successivi aggiornamenti/integrazioni;
2. assicurarsi che i dipendenti e collaboratori delle Strutture osservino tutte le disposizioni e istruzioni di cui al precedente punto 1;
3. adottare le opportune misure di sicurezza per garantire la protezione dei dati personali trattati;
4. provvedere alla redazione e all'aggiornamento, per la parte di competenza, del Registro delle attività di trattamento dell'Università di cui all'articolo 18 del presente Regolamento;
5. curare, nell'ambito di propria competenza, la redazione e l'aggiornamento delle informative e comunicazioni da fornire all'interessato sul trattamento dei dati personali ai sensi degli articoli 13 e 14 del Regolamento UE, da pubblicare, previo parere favorevole dell'Ufficio Privacy, nell'apposita pagina del sito web dell'Università;
6. tenere ed aggiornare gli archivi di dati personali, cartacei ed informatizzati nonché i server attivi eventualmente gestiti in maniera autonoma, ivi incluso cancellando o anonimizzando i dati personali quando non più necessari al raggiungimento delle finalità per i quali erano stati raccolti e, comunque, entro i termini di cancellazione previsti dalle policy dell'Università e/o da specifiche disposizioni normative e regolamentari;
7. segnalare con tempestività al Responsabile della Protezione dei Dati dell'Università e al Titolare del Trattamento eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di consentire l'effettuazione delle dovute valutazioni del caso e porre in essere gli adempimenti conseguenti. Nello specifico caso di violazione di dati personali, si rinvia a quanto disposto al successivo articolo 35.

9.3 I Responsabili Privacy hanno altresì il compito di vigilare e monitorare, qualora presenti all'interno delle Strutture, i rispettivi Referenti e, per il tramite di questi, gli Autorizzati al Trattamento, come individuati ai successivi articoli 11 e 12 del presente Regolamento.

9.4 Per l'attuazione dei compiti e degli adempimenti di cui al precedente comma 2, l'Ufficio Privacy e, se necessario, l'RPD assicureranno il necessario supporto.

Articolo 10
Poteri di sottoscrizione di atti e documenti relativi al trattamento dei dati personali

10.1 Fatto salvo quanto previsto al precedente articolo 8, comma 1, il presente Regolamento riconosce ai soggetti individuati al precedente articolo 9, comma 1, anche tenuto conto dell'eventuale autonomia gestionale e amministrativa ed esclusivamente per il proprio ambito di competenza, il potere di sottoscrizione dei seguenti atti e documenti relativi al trattamento dei dati personali:

i. atti di nomina a responsabile del trattamento redatti ai sensi e per gli effetti di cui all'articolo 28 del Regolamento UE, come individuati dall'articolo 14 del presente Regolamento;
ii. accordi di contitolarità redatti ai sensi e per gli effetti di cui all'articolo 26 del Regolamento UE e come individuati dall'articolo 13 del presente Regolamento;
iii. valutazioni di impatto (c.d. *Data Protection Impact Assessment*) redatte ai sensi e per gli effetti di cui all'articolo 35 del Regolamento UE e come individuate al successivo articolo 19 del presente Regolamento.

10.2 Per la stesura e/o la revisione degli atti e dei documenti di cui al precedente comma 1, l'Ufficio Privacy e, se necessario, l'RPD assicureranno il necessario supporto.

Articolo 11
Referenti dei trattamenti e compiti

11.1 Nell'ambito della propria organizzazione, il Titolare del Trattamento individua i Referenti che hanno il compito garantire il rispetto delle norme vigenti, del presente Regolamento e delle istruzioni impartite direttamente dal Titolare del Trattamento e/o per il tramite dei rispettivi Responsabili Privacy in materia di protezione dei dati personali secondo quanto disposto al successivo comma 3.

11.2 Sono individuati quali Referenti, in ragione delle specifiche funzioni, compiti e responsabilità a essi riconosciuti nell'ambito dell'attuale assetto organizzativo dell'Università, i seguenti soggetti:

a. i Capi degli Uffici dell'Amministrazione Centrale;
b. i Capi degli Uffici Dipartimentali;
c. i Capi degli Uffici delle Scuole;
d. i Direttori di Biblioteca di Area;
e. i professori e i ricercatori, nella qualità di responsabili scientifici di progetti di ricerca, qualora questi ultimi comportino il trattamento di dati personali;
f. ove presenti, i Responsabili dei processi amministrativi-contabili e i Direttori Tecnici delle Strutture decentrate, per gli ambiti di rispettiva competenza.

11.3 I Referenti, nell'ambito delle rispettive Strutture, autonomamente, congiuntamente o supportando i rispettivi Responsabili Privacy, sono tenuti a:

1. conoscere e rispettare le disposizioni del Regolamento UE, del Codice Privacy, del presente Regolamento, le istruzioni impartite dal Titolare del Trattamento in materia di protezione dei dati personali attraverso il Disciplinare attualmente vigente ed i loro successivi aggiornamenti/integrazioni;

2. assicurarsi che tutti i dipendenti e collaboratori afferenti alla Struttura di propria competenza osservino tutte le disposizioni e istruzioni di cui al precedente punto 1;
3. adottare le opportune misure di sicurezza per garantire la protezione dei dati personali trattati;
4. provvedere alla redazione e all'aggiornamento, per la parte di competenza, del Registro delle attività di trattamento dell'Università di cui all'articolo 18 del presente Regolamento;
5. curare, nell'ambito di propria competenza, la redazione e l'aggiornamento delle informative e comunicazioni da fornire all'interessato sul trattamento dei dati personali di cui agli articoli 13 e/o 14 del Regolamento UE, da pubblicare, previo parere favorevole dell'Ufficio Privacy, nell'apposita pagina del sito web dell'Università;
6. tenere ed aggiornare gli archivi di dati personali, cartacei ed informatizzati nonché i server attivi eventualmente gestiti in maniera autonoma, ivi incluso cancellando/distruggendo o anonimizzando i dati personali quando non più necessari al raggiungimento delle finalità per i quali erano stati raccolti e, comunque, cancellare/distruggere i dati personali entro i termini previsti dalle policy dell'Università e/o da specifiche disposizioni normative e regolamentari;
7. segnalare con tempestività al Responsabile della Protezione dei Dati dell'Università e al Titolare del Trattamento eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di consentire l'effettuazione delle dovute valutazioni del caso e porre in essere gli adempimenti conseguenti. Nello specifico caso di violazione di dati personali, si rinvia a quanto disposto al successivo articolo 35.

Articolo 12
Autorizzati al trattamento

12.1 I Responsabili Privacy e i Referenti, nell'ambito delle rispettive Strutture/ruoli, provvedono a individuare per iscritto – attualmente tramite i modelli Sicurdat – gli autorizzati a cui sono attribuiti specifici compiti e funzioni connessi ai trattamenti di propria competenza tra il personale tecnico-amministrativo, i docenti, i ricercatori, gli assegnisti di ricerca e i dottorandi dell'Università. Eventuali delegati del Rettore vengono individuati per iscritto da quest'ultimo.

12.2 Ciascun Autorizzato al Trattamento: (i) tratta i dati personali di titolarità dell'Università solo ed esclusivamente per le finalità connesse allo svolgimento delle mansioni o attività ad egli attribuite; (ii) deve osservare le disposizioni contenute nel presente Regolamento, nel Disciplinare attualmente in vigore nonché le ulteriori indicazioni fornite dai rispettivi Responsabili Privacy/Referenti; (iii) deve effettuare le attività di trattamento in osservanza delle misure di sicurezza adottate dall'Università e (iv) riceve formazione in materia di protezione dei Dati Personali.

12.3 L'Autorizzato al Trattamento è tenuto a:

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;

b) segnalare con tempestività al proprio Referente e al proprio Responsabile Privacy eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di consentire agli Uffici competenti e al Responsabile per la Protezione dei Dati personali di effettuare le dovute valutazioni del caso e porre in essere gli adempimenti conseguenti.

12.4 L'Autorizzato al Trattamento che abbia accesso ai sistemi informativi dell'Università è informato e consapevole che l'accesso e la permanenza in detti sistemi per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio, salvo le più gravi sanzioni

da rinvenirsi nell'ambito degli specifici ordinamenti, può comportare sanzioni disciplinari, oltre che esporre l'amministrazione a danni reputazionali.

12.5 Fermo restando quanto stabilito al primo comma del presente articolo, sono da considerarsi inoltre autorizzati anche tutti gli altri soggetti che, nell'ambito dell'assetto organizzativo del Titolare del Trattamento, per gli specifici compiti attribuiti/conferiti, abbiano accesso ai dati personali. Pertanto gli stessi sono designati autorizzati al trattamento dei dati personali e ricevono apposite istruzioni dal Titolare del Trattamento, per il tramite delle Strutture/degli Uffici competenti. I soggetti di cui al presente comma sono, in ogni caso, tenuti a conoscere e rispettare le disposizioni del Regolamento UE, del Codice Privacy, del presente Regolamento, le istruzioni impartite dal Titolare del Trattamento in materia di protezione dei dati personali attraverso il Disciplinare attualmente vigente ed i loro successivi aggiornamenti/integrazioni.

Articolo 13
Contitolari del trattamento

13.1 Quando l'Università determina le finalità e i mezzi del trattamento congiuntamente ad altro/i titolare/i del trattamento, pubblico o privato, assume, unitamente a questo/i ultimo/i, il ruolo di contitolare del trattamento.

13.2 I contitolari determinano in modo trasparente, mediante uno specifico accordo scritto, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui al successivo articolo 17.
Il contenuto essenziale dell'accordo di contitolarità è messo a disposizione dell'interessato, così come espressamente previsto dall'articolo 26, paragrafo 2 del Regolamento UE.

13.3. Per la stesura e/o la revisione dell'accordo di cui al precedente comma 2, l'Ufficio Privacy dell'Università e, se necessario, l'RPD assicureranno il necessario supporto.

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

Articolo 14
Responsabile del trattamento

14.1 Il responsabile del trattamento è il soggetto esterno all'organizzazione dell'Università che effettua trattamenti per conto dell'Università stessa.

14.2 L'Università ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE e garantisca la tutela dei diritti dell'interessato.

14.3 Il Responsabile del trattamento è nominato con un contratto o altro atto giuridico in cui sono disciplinati, tra l'altro, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, le responsabilità

e le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste dal Regolamento UE.

14.4 Per specifiche attività di trattamento e nel rispetto degli obblighi contrattuali che lo legano all'Università, il Responsabile del Trattamento può nominare sub-responsabili del trattamento esclusivamente previa autorizzazione scritta, specifica o generale, dell'Università e con attribuzione al sub-responsabile dei medesimi obblighi in materia di protezione dei dati personali derivanti dal contratto – o altro atto giuridico – stipulato con l'Università. Così come espressamente previsto dall'articolo 28, paragrafo 4, del Regolamento UE, qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dati, il responsabile del trattamento iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.

14.5 L'Università può essere nominata responsabile del trattamento di uno o più trattamenti per conto di un altro titolare del trattamento.

Articolo 15
Responsabile della Protezione dei Dati

15.1 Il Responsabile della Protezione dei Dati è nominato tra il personale di alta qualificazione dell'Università, in funzione delle qualità professionali e della capacità di assolvere ai compiti di cui al successivo comma 2.

15.2 Il Titolare del trattamento designa il Responsabile della Protezione dei Dati per lo svolgimento dei seguenti compiti:

a) informare e fornire consulenza al Titolare del Trattamento, ai Responsabili del Trattamento, ai Referenti interni e ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati;
b) sorvegliare l'osservanza della normativa in materia di protezione dei dati nonché delle politiche in materia di protezione dei dati del Titolare del Trattamento, del Responsabile del trattamento e dei Referenti, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire pareri in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento all'interno dell'Università;
d) cooperare e fungere da punto di contatto con l'Autorità Garante in merito alle questioni connesse al trattamento dati.

15.3 Il provvedimento di nomina del Responsabile della Protezione dei Dati può indicare ulteriori e più specifici compiti.

15.4 Il Titolare del Trattamento assicura che il Responsabile della Protezione dei Dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

15.5 Il Responsabile della Protezione dei Dati opera in posizione di autonomia e indipendenza; il Titolare del Trattamento assicura che il Responsabile della Protezione dei Dati non riceva alcuna istruzione per l'esecuzione dei suoi compiti.

15.6 Il Responsabile della Protezione dei Dati può essere contattato dagli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dalla normativa in materia di protezione dei dati personali.

15.7 I dati di contatto del Responsabile della Protezione dei Dati sono pubblicati sul sito dell'Università e comunicati all'Autorità Garante in base alla procedura informatizzata predisposta dallo stesso.

Articolo 16
Amministratori di Sistema

16.1 Sono amministratori di sistema, ai sensi del Provvedimento dell'Autorità Garante del 27 novembre 2008 e ss.mm.ii. le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente Regolamento sono da considerarsi tali anche gli amministratori di basi di dati, gli amministratori di rete, gli amministratori di apparati di sicurezza, gli amministratori di sistemi software complessi.

16.2 Ai fini del rispetto delle prescrizioni dell'Autorità Garante, l'Ufficio Privacy, per conto dell'Ateneo, custodisce l'elenco degli amministratori di sistema in un documento. Il documento deve essere regolarmente aggiornato dal Centro Servizi Informativi di Ateneo e disponibile in caso di accertamenti da parte dell'Autorità Garante.

16.3 A tal fine, l'Ufficio Privacy riceve dal Centro Servizi Informativi di Ateneo le comunicazioni delle modificazioni intervenute.

CAPO IV
ADEMPIMENTI

Articolo 17
Informativa

17.1 L'Università, quando effettua un trattamento di dati personali, fornisce apposita informativa all'interessato, salvo il caso in cui quest'ultimo sia già in possesso delle informazioni o nei casi particolari previsti al successivo comma 4.

17.2 L'informativa fornita all'interessato deve essere concisa, trasparente, intellegibile, facilmente accessibile ed essere formulata con un linguaggio semplice e chiaro.

17.3 L'informativa deve contenere:

a) i dati di contatto dell'Università;
b) i dati di contatto del Responsabile della Protezione dei Dati;
c) la finalità per cui sono trattati i dati personali;
d) la condizione di liceità che legittima il trattamento;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) l'eventuale intenzione dell'Università di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, con indicazione del fondamento giuridico del trasferimento (esistenza di una decisione di adeguatezza della Commissione Europea o garanzie appropriate o opportune) e indicazione dei mezzi per ottenere una copia dei dati o del luogo dove sono stati resi disponibili;
g) il periodo di conservazione dei dati personali oppure, se non è possibile indicare il periodo, i criteri utilizzati per determinarlo;
h) i diritti dell'interessato;
i) la natura obbligatoria o facoltativa della fornitura dei dati e le possibili conseguenze del mancato conferimento;
j) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione, con indicazioni sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato;
k) il diritto di proporre reclamo a un'autorità di controllo.

17.4 Se la raccolta dai dati non avviene presso l'interessato, l'Università fornisce al medesimo, in aggiunta alle indicazioni di cui al precedente comma 3, le seguenti informazioni:
a) le categorie di dati trattati;
b) la fonte da cui i dati hanno origine.

Ai sensi dell'articolo 14, paragrafo 5 del Regolamento UE, le informazioni di cui al presente comma e al precedente comma 3, non devono essere fornite dall'Università se, a valle di opportune valutazioni da effettuarsi anche congiuntamente all'Ufficio Privacy e all'RPD:

i. comunicare tali informazioni all'interessato risulti impossibile o implicherebbe uno sforzo sproporzionato per l'Università, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie individuate al successivo articolo 28 o nella misura in cui l'obbligo di comunicare le informazioni di cui al presente articolo rischi di rendere impossibile o pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, l'Università deve adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche informazioni (ad esempio, sui propri canali istituzionali);
ii. l'ottenimento o la comunicazione dei dati personali sono espressamente previsti dal diritto dell'Unione Europea o dal diritto nazionale, che prevede misure appropriate per tutelare gli interessi legittimi degli interessati;
iii. i dati personali devono rimanere riservati conformemente ad un obbligo di segretezza previsto dalla legge.

17.5 Qualora l'Università intenda trattare i dati per una finalità differente da quella per cui sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito alla diversa finalità e ogni ulteriore informazione pertinente.

17.6 Ogni singola Struttura dell'Università assolve agli obblighi di informativa previsti dal Regolamento UE con il supporto dell'Ufficio Privacy e, qualora necessario, previo parere dell'RPD.

Articolo 18
Registro delle attività di trattamento

18.1 L'Università tiene e aggiorna il Registro delle attività di Trattamento, che è un documento scritto di censimento e analisi dei trattamenti effettuati dalla stessa o in qualità di titolare del trattamento o in qualità di responsabile del trattamento. L'Università si è dotata di un registro scritto in formato elettronico.

18.2 Il Registro delle attività di Trattamento di cui al precedente comma 1, redatto dall'Università quale Titolare del Trattamento, contiene le seguenti informazioni, come previsto dall'articolo 30 del Regolamento UE:

a) dati identificativi e di contatto dell'Università, degli eventuali Contitolari e dell'RPD;
b) dati identificativi dei Referenti di Struttura, automaticamente importati dalla piattaforma CSA (Gestione Carriere e Stipendi) in uso presso l'Università;
c) i dati identificativi dei soggetti delegati (c.d. unità di delega privacy), competenti a fornire supporto al Referente di Struttura per la redazione del registro delle attività di trattamento e individuati dallo stesso Referente di Struttura tra le unità di personale tecnico amministrativo incardinate presso la Struttura di riferimento;
d) le finalità del Trattamento;
e) la descrizione delle categorie degli Interessati e delle categorie di Dati Personali;
f) le categorie di destinatari, a cui i Dati Personali sono stati o saranno comunicati, compresi destinatari di paesi terzi od organizzazioni internazionali;
g) l'eventuale trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, indicando i dati identificativi del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al successivo articolo 23 punto ii., la documentazione delle garanzie adeguate;
h) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
i) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate, che comprendono, tra le altre, se del caso, quelle previste dall'articolo 34 del presente Regolamento.

18.3 L'Università tiene e aggiorna, inoltre, il Registro delle attività di Trattamento in qualità di Responsabile del Trattamento, nel quale sono descritte le attività di Trattamento svolte per conto di altri Titolari del Trattamento, che deve contenere le seguenti informazioni:

a) dati identificativi e di contatto dell'Università, del Titolare del Trattamento per conto del quale agisce l'Università, di eventuali altri Responsabili del Trattamento e dell'RPD dell'Università e del Titolare del Trattamento per conto del quale agisce l'Università;
b) le categorie di Trattamenti effettuati per conto di ogni Titolare del Trattamento;
c) l'eventuale trasferimento 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 successivo articolo 23 la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate di cui all'articolo 34 del presente Regolamento.

18.4 Ciascuna Struttura, per il tramite del proprio Referente, come individuato dall'articolo 11 del presente Regolamento, redige i Registri delle attività di Trattamento di cui ai precedenti commi 2 e 3, in collaborazione con l'Ufficio Privacy, e ne cura periodicamente l'aggiornamento. I Registri delle attività di Trattamento devono essere messi a disposizione dell'Autorità Garante su richiesta di quest'ultima.

Articolo 19
Valutazione d'impatto sulla protezione dei dati
(o *Data Protection Impact Assessment*)

19.1 L'Università effettua una valutazione d'impatto sulla protezione dei dati (o "*data protection impact assessment*" – c.d. "DPIA") quando le attività di Trattamento dei Dati Personali poste in essere in qualità di Titolare del Trattamento, che prevedono in particolare l'utilizzo di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del Trattamento, possono presentare un rischio elevato per i diritti e le libertà dell'interessato. Una singola valutazione d'impatto può essere effettuata per un insieme di trattamenti simili che presentano rischi elevati analoghi.

19.2. Ai sensi dell'articolo 35 del Regolamento UE, la valutazione d'impatto è obbligatoria, in particolare, nei casi seguenti:

a) valutazione sistematica e globale degli 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) 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 o a connesse misure di sicurezza;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza).

19.3 In aggiunta ai casi di cui al precedente comma 2, è altresì obbligatorio condurre una valutazione d'impatto quando il trattamento di dati personali posto in essere dall'Università possa presentare un rischio elevato per i diritti e le libertà degli interessati, considerando i seguenti criteri individuati dal Comitato Europeo di Protezione dei Dati Personali (già *Working Party* 29) nelle Linee Guida in materia adottate il 4 aprile 2017:

1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sugli interessati;
3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
4. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite al successivo articolo 26, nonché dati personali relativi a condanne penali o reati, come definiti al successivo articolo 27; trattamento di dati su larga scala. Al fine di stabilire se un trattamento sia effettuato su larga scala, si deve tener conto: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento;

5. creazione di corrispondenze o combinazione di insiemi di dati;
6. dati relativi a interessati vulnerabili. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;
7. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
8. quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

19.4 In aggiunta ai casi di cui al precedente comma 2 e ai criteri di cui al precedente comma 3, è altresì obbligatorio condurre una valutazione d'impatto nei seguenti casi individuati dall'Autorità Garante con Provvedimento n. 467 dell'11 ottobre 2018:

1. trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
2. trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere;
3. trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app;
4. trattamenti su larga scala di dati aventi carattere estremamente personale;
5. trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;
6. trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
7. trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo;
8. trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
9. trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni;
10. trattamenti di categorie particolari di dati come individuati al successivo articolo 26 oppure di dati relativi a condanne penali e a reati di cui al successivo articolo 27 interconnessi con altri dati personali raccolti per finalità diverse;
11. trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;
12. trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

19.5 L'Università, attraverso le Strutture coinvolte nei singoli trattamenti, con la collaborazione del RPD, determina i casi nei quali si rende necessario procedere a una valutazione di impatto nel rispetto di quanto previsto dai precedenti commi 2, 3 e 4. Una volta effettuata la valutazione d'impatto, la documentazione, come previsto al precedente articolo 10, deve essere sottoscritta dal relativo Responsabile Privacy, come individuato al precedente articolo 9, e controfirmata dall'RPD.

19.6 Nei casi in cui, al termine della valutazione di impatto e dell'adozione delle misure di sicurezza, si ritenesse che le attività di trattamento comportino un rischio residuo elevato per gli interessati, il Titolare del Trattamento, in collaborazione con l'RPD, procederà a consultare l'Autorità Garante ai sensi dell'articolo 36 del Regolamento UE.

CAPO V
DIRITTI DELL'INTERESSATO

Articolo 20
Diritti dell'interessato

20.1 L'Università garantisce il rispetto dei diritti degli interessati disciplinati dagli articoli da 15 a 22 del Regolamento UE, ove applicabili.

20.2 In particolare, fatte salve le previsioni di legge, l'interessato ha il diritto di:

a) avere conferma dal Titolare del Trattamento che sia o meno in corso un'attività di Trattamento sui propri Dati Personali e ottenere l'accesso a tali dati ("diritto di accesso ai dati personali");

b) ottenere la rettifica dei dati inesatti e l'integrazione dei dati incompleti ("diritto alla rettifica");

c) ottenere la cancellazione dei propri Dati Personali ("diritto alla cancellazione" o "diritto all'oblio");

d) ottenere la limitazione al trattamento dei propri dati ("diritto di limitazione");

e) ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i relativi Dati Personali forniti a un Titolare del Trattamento e trasmettere tali dati a un altro Titolare del Trattamento senza impedimenti da parte del Titolare del Trattamento cui li ha forniti ("diritto alla portabilità");

f)opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al Trattamento dei propri Dati Personali ai sensi dell'articolo 6, paragrafo 1, lett. e) o f), del Regolamento UE, compresa la Profilazione ("diritto di opposizione");

g) opporsi in qualsiasi momento al trattamento dei dati personali che riguardano la sua situazione particolare anche quando il trattamento è stato effettuato per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero per i legittimi interessi di un titolare del trattamento o di terzi ("diritto di opposizione");

h) non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione, che produca effetti giuridici nei confronti dell'interessato stesso o che incida in modo analogo significativamente sulla propria persona, fatti salvi i casi in cui ciò è previsto dalla legge ("diritto a non essere sottoposti a trattamento automatizzato").

20.3 L'Interessato presenta istanza di esercizio dei diritti preferibilmente attraverso i canali di contatto dedicati, senza alcuna formalità, previa dimostrazione della propria identità.

20.4 L'Università risponde tempestivamente alle richieste di esercizio dei diritti e, comunque, entro un mese dal ricevimento dell'istanza. Tale termine può essere prorogato di ulteriori due mesi (per un totale di tre mesi), tenuto conto della complessità e del numero delle richieste. In ogni caso, l'Università dovrà comunicare tale proroga all'Interessato entro un mese dal ricevimento dell'istanza, indicando i motivi del ritardo.

20.5 L'Università può negare la risposta a una richiesta di esercizio dei diritti solo nel caso in cui quest'ultima risulti manifestamente infondata o eccessiva, in particolare per il suo carattere ripetitivo; sarà onere dell'Università dimostrare il carattere manifestamente infondato o eccessivo della richiesta e comunicare i motivi del diniego all'Interessato.

20.6 L'Università non richiede un contributo spese all'interessato per dare riscontro alle richieste di esercizio dei diritti di quest'ultimo, fatti salvi i casi di istanze manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo.

CAPO VI
CIRCOLAZIONE, COMUNICAZIONE E TRASFERIMENTO DI DATI PERSONALI

Articolo 21
Circolazione dei dati personali all'interno dell'Università

21.1 Il trattamento dei dati personali da parte delle Strutture dell'Università è comunque limitato ai casi in cui sia finalizzato al perseguimento delle finalità istituzionali e dei compiti ad esse connesse.

21.2 L'accesso ai dati personali da parte delle Strutture e del personale dell'Università è ispirato, tra l'altro, al principio di minimizzazione. Pertanto, le informazioni devono essere rese disponibili esclusivamente ai soggetti che hanno necessità di accedervi per lo svolgimento dell'attività lavorativa.

Articolo 22
Comunicazione e diffusione dei dati personali

22.1 La comunicazione di dati personali è un'operazione di trattamento che consiste nel portare i dati personali a conoscenza di uno o più soggetti identificabili in modo univoco e determinato. Non si considera comunicazione lo scambio di dati tra: (i) Strutture interne dell'Università; (ii) tra l'Università e soggetti esterni individuati come responsabili del trattamento; (iii) soggetti Autorizzati al Trattamento.

22.2 La comunicazione dei dati personali, come individuata al precedente comma 1, può avvenire solo ove sussista una delle condizioni di liceità tra quelle di cui all'articolo 7 del presente Regolamento.

22.3 La diffusione è un'operazione di trattamento che consiste nel portare i dati personali a conoscenza di soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La diffusione è consentita soltanto in presenza di una valida condizione di liceità tra

quelle di cui all'articolo 7 del presente Regolamento, sempre nel rispetto del principio di minimizzazione, dei principi legislativi nonché dei provvedimenti dell'Autorità Garante di volta in volta applicabili.

Articolo 23
Trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale

Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale situati al di fuori dello Spazio Economico Europeo (s'intende per Spazio Economico Europeo o "SEE" il territorio degli Stati Membri dell'Unione Europea, Islanda, Liechtenstein e Norvegia), l'Università è responsabile del rispetto delle specifiche condizioni disciplinate nel Capo V del Regolamento UE, affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dallo stesso. Pertanto, l'Università può trasferire dati personali al di fuori dello Spazio Economico Europeo solo in presenza delle seguenti condizioni:

i. decisioni di adeguatezza adottate dalla Commissione Europea nei confronti del Paese terzo o dell'organizzazione internazionale, come espressamente previsto dall'articolo 45 del Regolamento UE;
ii. garanzie adeguate rilasciate dal soggetto terzo destinatario ai sensi dell'articolo 46 del Regolamento UE.

Articolo 24
Diritto d'accesso, accesso civico e riservatezza

Per i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso a documenti amministrativi e del diritto di accesso civico, con riferimento ai dati personali di terzi, si rinvia al Regolamento di Ateneo in materia di diritto di accesso e alle disposizioni normative in materia nel tempo vigenti, anche con riferimento ai tipi di dati di cui agli articoli 9 e 10 del Regolamento UE.

TITOLO III
TRATTAMENTI DI DATI PERSONALI

Articolo 25
Tipologie di dati personali trattati dall'Università

25.1 L'Università effettua, con misure adeguate e tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto, delle finalità del trattamento, trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali, come individuate da disposizioni di legge, statutarie e regolamentari e nei limiti imposti dal Codice Privacy, dal Regolamento UE e dalle Linee guida e dai provvedimenti dell'Autorità Garante.

25.2 L'Università effettua, a titolo esemplificativo e non esaustivo, i seguenti trattamenti di dati personali previsti dalla normativa nazionale e interna di Ateneo riguardanti:

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

- gestione del rapporto di lavoro;
- gestione economica, fiscale, previdenziale e assistenziale;
- gestione degli infortuni;
- formazione e aggiornamento professionale;
- politiche Welfare e per la fruizione di agevolazioni;
- salute e la sicurezza delle persone nei luoghi di lavoro;
- accesso ad aree riservate e parcheggi di pertinenza dell'Ateneo;
- smart working e telelavoro;
- erogazione del servizio di telefonia fissa e mobile.

b) Dati, anche di natura particolare, relativi a studenti, ivi compresi coloro che hanno già terminato gli studi e categorie assimilate. Tali dati vengono trattati nell'ambito delle seguenti attività:

- 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*;
- rilevazioni statistiche e valutazione della didattica;
- servizi di tutorato, assistenza, inclusione sociale;
- servizi e attività per il diritto allo studio;
- servizi di assistenza ai diversamente abili e DSA;

c) Dati relativi alla didattica e alla ricerca. Tali dati vengono trattati, tra l'atro, nell'ambito delle seguenti attività:

- gestione di progetti di ricerca;
- trasferimento tecnologico;
- monitoraggio e valutazione della ricerca.

d) Dati relativi alle attività gestionali interne all'Università e alle attività svolte per conto terzi e/o connessi ad attività trasversali:

- gestione degli spazi;
- gestione delle postazioni;
- gestione degli organi e delle cariche istituzionali;
- 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 istituzionale;
- videosorveglianza.

25.3 Si intendono comunque disciplinati dal presente Regolamento tutti i trattamenti di dati posti in essere dall'Università, anche se non presenti nell'elenco di cui al precedente comma 2, che rientrino nello svolgimento dei compiti istituzionali dell'Università stessa o che siano ad essa prescritti da una norma di legge.

Articolo 26
Trattamento di categorie particolari di dati personali

26.1 Si considerano, ai sensi dell'articolo 9 del Regolamento UE, categorie particolari di dati personali quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco

una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

26.2 L'Università può trattare i dati personali di cui al precedente comma 1 solo in presenza di una delle condizioni di seguito elencate:

a) l'interessato ha prestato il consenso esplicito per una o più finalità specifiche;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti dell'Università o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
c) il trattamento è necessario per tutelare un interesse vitale della persona interessata o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestatamente pubblici dall'interessato;
e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
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 e i dati sono trattati da o sotto la responsabilità di un professionista soggetto a segreto professionale;
g) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, in conformità al successivo articolo 28;
h) il trattamento è necessario per motivi di interesse pubblico rilevante, se previsto dal diritto dell'Unione Europea o da una disposizione di legge o di regolamento 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.

Articolo 27
Trattamento di dati personali relativi a condanne penali e reati

L'Università può trattare Dati Personali Giudiziari esclusivamente in presenza di una norma di legge o, nei casi previsti dalla legge, di regolamento, che autorizzi tale trattamento in particolare nei seguenti casi:

a) adempimento di obblighi ed esercizio di diritti da parte del Titolare del Trattamento o dell'interessato nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del Regolamento UE;
b) adempimento di obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione di controversie civili e commerciali;
c) verifica o accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
d) accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
e) accertamento, esercizio o difesa di un diritto in sede giudiziaria;
f) esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
g) adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi

forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;

h) accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;

i) adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Articolo 28
Trattamento a fini di archiviazione, di ricerca scientifica o storica e a fini statistici

28.1 L'Università, nel trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica e a fini statistici, predispone misure tecniche e organizzative che garantiscano il rispetto del principio della minimizzazione dei dati, ivi inclusa la pseudonimizzazione e l'anonimizzazione, se le finalità del trattamento possono essere raggiunte mediante tali misure.

28.2 Con specifico riferimento al trattamento dei dati personali effettuato nell'ambito dei progetti di ricerca, il relativo Referente, come individuato all'articolo 11, comma 2, lettera d), del presente Regolamento, dovrà trasmettere all'Ufficio Privacy dell'Università:

a) la Scheda per l'analisi dei rischi dei progetti di ricerca, disponibile sul sito web istituzionale dell'Università, descrivendo dettagliatamente: finalità e modalità del trattamento; natura dei dati, luogo dove sono custoditi, categorie di interessati cui i dati si riferiscono; ambito di comunicazione e diffusione dei dati; una descrizione delle misure di sicurezza adottate; eventuale connessione con altri trattamenti o banche dati;

b) la Dichiarazione di impegno a cura del/della Responsabile del progetto di ottemperanza alle disposizioni delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica del 19 dicembre 2018, ai sensi dell'art. 20, comma 4, del D. Lgs. n. 101/2018;

c) qualsiasi altra documentazione utile ai fini della valutazione del trattamento dei dati personali nell'ambito del progetto di ricerca.

28.3 L'Università deve fornire all'interessato puntuale informativa relativamente al trattamento per finalità statistiche o di ricerca scientifica, a meno che questo non richieda uno sforzo sproporzionato rispetto al diritto tutelato e sempre che siano adottate le idonee forme di pubblicità individuate dalle regole deontologiche in materia.

28.4 Il trattamento è effettuato nel rispetto delle regole deontologiche in materia approvate dall'Autorità Garante.

Articolo 29
Trattamento a fini di ricerca medica, biomedica ed epidemiologica

29.1 Fatto salvo quanto previsto dal precedente articolo 28, le Strutture dell'Università che, nell'ambito delle proprie finalità istituzionali, effettuino un trattamento di dati personali a fini di ricerca medica, biomedica ed epidemiologica, individuano, con il supporto dell'RPD, idonea condizione di liceità e pongono in essere tutti gli adempimenti prescritti dalla normativa applicabile, ivi inclusa, se necessario, la redazione di una valutazione d'impatto, ai sensi dell'articolo 19 del presente Regolamento.

29.2 Ai sensi e per gli effetti di cui all'articolo 110 del Codice Privacy, il consenso dell'interessato al trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico ed epidemiologico non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione Europea - ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-*bis* del Decreto Legislativo n. 502/1992 (Ricerca sanitaria) - ed è condotta e resa pubblica una valutazione d'impatto.

29.3 Il consenso al trattamento non è necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il Titolare adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato; il programma di ricerca è oggetto di motivato parere favorevole del Comitato Etico a livello territoriale e deve essere sottoposto a valutazione d'impatto sulla protezione dei dati secondo quanto previsto dall'articolo 19 del presente Regolamento.

29.4 In caso di esercizio del diritto di rettifica e integrazione dei dati personali da parte dell'interessato, la rettificazione e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

Articolo 30
Trattamento nell'ambito di rapporti di lavoro

30.1 L'Università tratta i dati personali del personale per la finalità di instaurazione, gestione e cessazione del rapporto di lavoro, adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli interessati, e nel rispetto della legge e, ove applicabile al tipo di rapporto, dei contratti collettivi.

30.2 Il trattamento non richiede il consenso dell'interessato, in quanto necessario per assolvere gli obblighi ed esercitare i diritti del Titolare del Trattamento e dell'interessato in materia di diritto del lavoro, sicurezza e protezione sociale.

30.3 Ove previsto dalla legge o, in assenza di questa, previa individuazione di un'idonea condizione di liceità, l'Università comunica a soggetti pubblici e privati i dati personali del personale a fini di gestione del rapporto di lavoro.

30.4 L'Università, ove previsto da una disposizione di legge o di regolamento (ad esempio, per adempiere a specifici obblighi di trasparenza), nel rispetto del principio di minimizzazione, diffonde i dati personali comuni del personale (ad esempio sul proprio sito web istituzionale).

Articolo 31
Trattamento dei dati personali degli studenti

Per agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, l'Università può comunicare, previa individuazione di una idonea condizione di liceità e nel rispetto del

principio di minimizzazione, anche a privati e per via telematica, dati personali degli studenti, ad esclusione delle categorie di dati personali di cui agli articoli 25 e 27 del presente Regolamento, pertinenti in relazione alle predette finalità e ai compiti ad esse connesse.

Articolo 32
Trattamento dei dati personali da parte dei componenti degli Organi, Gruppi di lavoro, Comitati e Commissioni a vario titolo istituite all'interno dell'Università

I componenti degli Organi, dei Gruppi di lavoro, dei Comitati e delle Commissioni a vario titolo istituite all'interno dell'Università trattano i dati personali in conformità alla normativa applicabile e al presente Regolamento, al solo fine dello svolgimento delle attività istruttorie necessarie per le finalità di competenza degli stessi.

I soggetti individuati al precedente comma 1 sono pertanto tenuti a:

1. conoscere e rispettare le disposizioni del Regolamento UE, del Codice Privacy, del presente Regolamento e del Disciplinare attualmente vigente per le parti applicabili e compatibili;
2. adottare le opportune misure di sicurezza per garantire la protezione dei dati personali trattati;
3. tenere e aggiornare gli archivi di dati personali, cartacei ed informatizzati nonché i server attivi eventualmente gestiti in maniera autonoma;
4. segnalare con tempestività al Responsabile della Protezione dei Dati dell'Università e al Titolare del Trattamento eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di consentire l'effettuazione delle dovute valutazioni del caso e porre in essere gli adempimenti conseguenti. Nello specifico caso di violazione dei dati personali, si rinvia a quanto disposto al successivo articolo 35.

Articolo 33
Videosorveglianza

33.1 L'Università può installare telecamere di videosorveglianza per finalità di: a) sicurezza e incolumità del personale universitario, degli studenti e dei frequentatori a vario titolo degli spazi universitari; b) tutela del patrimonio immobiliare dell'Ateneo; c) tutela dei beni mobili dell'Università e degli utenti; d) prevenzione di atti vandalici; accesso a varchi o proprietà di diretta pertinenza dell'Ateneo.

33.2 Prima di procedere all'installazione di un impianto di videosorveglianza o di una nuova telecamera, il Referente della Struttura dovrà inoltrare richiesta alla Direzione Generale mediante l'apposito modello, disponibile sul sito web istituzionale dell'Università, completo di tutte le informazioni e i documenti necessari. La Direzione Generale, con il supporto delle Aree e degli Uffici competenti, previa preliminare valutazione circa l'esistenza dei presupposti, avvia, nel rispetto delle disposizioni legislative e contrattuali contenute nel CCNL comparto Istruzione e Ricerca, il sistema delle relazioni sindacali con le OO.SS e con le RSU.

33.3 Non si potrà procedere all'installazione delle telecamere se la procedura indicata al comma precedente non risulti completa o l'accordo sindacale non sia andato a buon fine.

33.4 L'Università può affidare le attività di videosorveglianza a soggetti terzi che saranno nominati, con apposito contratto o altro atto giuridico, Responsabili del Trattamento.
Qualora l'attività di videosorveglianza sia assicurata anche mediante la visualizzazione delle immagini da parte del personale tecnico amministrativo dell'Università, i Referenti di cui all'articolo 11 del

presente Regolamento sono tenuti a nominare gli autorizzati individuati tra il personale in servizio presso la propria unità organizzativa mediante compilazione del modello "SICURDAT VIDEO", reperibile sul sito web istituzionale dell'Università e a trasmettere tale modello all'Ufficio Privacy mediante protocollo informatico.

TITOLO IV
MISURE DI SICUREZZA E DATA BREACH

Articolo 34
Misure di sicurezza

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

34.2 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.

34.3 Per quanto non espressamente disciplinato dal presente articolo, si fa rinvio a quanto disposto dal *Disciplinare per l'utilizzo nel rapporto di lavoro anche a distanza degli strumenti informatici e telematici* reperibile sul sito web dell'Università, nonché dalle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte dall'Agenzia per l'Italia Digitale (AgID).

Articolo 35
Violazione dei dati personali (c.d. "Data Breach")

35.1 Per violazione dei dati personali si intende una violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati può, se non affrontata in modo adeguato e tempestivo, provocare danni rilevanti agli interessati, quali, ad esempio, il furto o l'usurpazione di identità, pregiudizio alla reputazione o qualsiasi altro danno economico o sociale significativo. Conseguentemente, la violazione può esporre l'Università a rischi significativi.

35.2 Pertanto, qualora si verifichi o si sospetti una violazione di dati personali il Referente o il Responsabile del trattamento dovranno darne immediata comunicazione al Responsabile della Protezione dei Dati dell'Università (RPD), notificando l'intervenuta violazione tempestivamente e comunque non oltre 12 ore dalla scoperta dell'evento, secondo la procedura prevista sul sito web istituzionale dell'Università.

35.3 Ove ne ricorrano i presupposti, il Titolare del Trattamento notifica la violazione all'Autorità Garante senza ritardo dal momento in cui ne è venuto a conoscenza, secondo quanto previsto dall'articolo 33 del Regolamento UE.

35.4 Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università, quale titolare del trattamento, comunica la violazione all'interessato senza ingiustificato ritardo, nel rispetto di quanto previsto dall'articolo 34 del Regolamento UE.

TITOLO V
DISPOSIZIONI FINALI

Articolo 36
Formazione

36.1 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 la diffusione dell'informativa a tutti coloro che hanno rapporti con l'Università.

36.2 L'Università organizza iniziative formative 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. Le iniziative in materia sono programmate annualmente, su proposta dell'RPD, nella specifica sezione del PIAO di Ateneo dedicata alla formazione del personale dirigenziale e tecnico-amministrativo, aggiornata a cura dell'Area Organizzazione e Sviluppo e dell'Ufficio Formazione. A cura di tale Ufficio viene effettuato un monitoraggio sulla formazione obbligatoria fruita in corso d'anno rispetto a quella programmata, di cui si tiene conto anche in sede di valutazione di una correlata voce di comportamento del personale dirigenziale e tecnico-amministrativo interessato.

Articolo 37
Violazioni del Regolamento

Le violazioni delle disposizioni del presente Regolamento in materia di trattamento dei dati personali, del Regolamento UE, del Codice Privacy nonché delle istruzioni impartite dal Titolare costituiscono violazioni degli obblighi di comportamento e saranno valutate quali ipotesi di responsabilità disciplinare secondo i principi e le modalità previste dagli specifici codici etici e di disciplina.