REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DELL'UNIVERSITÀ DI FOGGIA

"I termini relativi a persone che, nel presente regolamento, compaiono solo al maschile si riferiscono indistintamente a persone di genere femminile e maschile. Si è rinunciato a formulazioni rispettose dell'identità di genere per non compromettere la leggibilità del testo e soddisfare l'esigenza di semplicità dello stesso."

INDICE

PARTE I
DISPOSIZIONI GENERALI
ART. 1
AMBITO DI APPLICAZIONE

1. Il presente Regolamento, adottato in attuazione del Regolamento (UE) 27 aprile 2016, n. 679 (di seguito, anche "GDPR") e del D. Lgs. n. 196/2003 come novellato dal D. Lgs. n. 101/2018 (di seguito, "Codice privacy") e successive modifiche ed integrazioni, disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi effettuati dall'Università degli Studi di Foggia.
2. L'Università degli Studi di Foggia (di seguito Università), come Pubblica Amministrazione ai sensi dell'art. 1, c. 2 del D. Lgs. n. 165/2001 e ss.mm.ii., persegue finalità di interesse pubblico come definite dalla legge e dal proprio Statuto.
3. L'Università, in qualità di Titolare del trattamento, tratta i dati personali dei soggetti interessati nell'ambito del perseguimento delle proprie finalità istituzionali, nel rispetto dei diritti e delle libertà fondamentali, della dignità e del diritto alla protezione dei dati personali degli individui, in modo da instaurare un rapporto di fiducia con gli studenti, il personale docente/ricercatori, il personale tecnico amministrativo e con coloro che, a vario titolo, entrano in contatto con l'Università stessa.
4. L'Università effettua il trattamento dei dati personali in conformità alla vigente disciplina europea e nazionale in materia di protezione dei dati personali.
5. Il trattamento dei dati personali avviene nel rispetto della normativa vigente, sulla base delle condizioni di liceità previste dal GDPR e dal Codice Privacy, come specificato nell'art. 4 del presente regolamento.

ART. 2
DEFINIZIONI

1. Ai fini del presente Regolamento ed in conformità a quanto previsto dalla normativa vigente nazionale ed europea 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 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 (art. 4, n. 2 del GDPR. Regolamento Generale sulla Protezione dei Dati Personali);

b) "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile (soggetto «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 (art. 4, n. 1 del GDPR);

c) "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, nonché trattare 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 (art. 9, par. 1, del GDPR);

d) "dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una

persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4, n. 13 del GDPR);

e) "dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (art. 4, n. 14 del GDPR);
f) "dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4, n. 15 del GDPR);
g) "dati giudiziari": i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR)
h) "consenso dell'interessato": manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva a inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
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 (art. 4, n. 7 del GDPR);
j) "contitolare del trattamento": il titolare del trattamento che con uno o più titolari determina congiuntamente le finalità e i mezzi del trattamento di dati personali;
k) "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 (art. 4, n. 8 del GDPR);
l) "responsabile della protezione dei dati" (di seguito, RPD): figura professionale esperta nella protezione dei dati con il compito di garantire la corretta applicazione della normativa europea e nazionale in materia di protezione dei dati all'interno di ciascuna organizzazione ove è designato (artt. 37, 38 e 39 del GDPR);
m) "responsabile per la transizione al digitale" (di seguito, RTD): figura istituita nelle pubbliche amministrazioni per garantire la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità (art. 17 del Codice dell'Amministrazione Digitale);
n) "autorizzato": il soggetto che agisce sotto l'autorità del titolare o del responsabile del trattamento e che ha accesso ai dati personali (art. 29 del GDPR);
o) "amministratore di sistema": nell'ambito del Provvedimento del Garante del 27 novembre del 2008 gli AdS sono individuati come una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
p) "comunicazione": dare conoscenza dei dati personali a uno o più soggetti determinati diversi dal soggetto interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

q) “diffusione”: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
r) “informazioni anonime”: informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione del soggetto interessato (Considerando 26 del GDPR);

Per tutte le altre definizioni relative al trattamento dei dati personali non comprese eventualmente nel presente articolo si rinvia alla normativa europea e nazionale in materia di protezione dei dati personali e alle linee guida del Garante Italiano per la Protezione dei Dati Personali e dello European Data Protection Board.

ART. 3
PRINCIPI RELATIVI AL TRATTAMENTO DEI DATI PERSONALI

1. L’Università di Foggia effettua il trattamento dei dati personali in applicazione dei principi previsti dagli artt.5 e 25 del GDPR.
2. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente (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 dei soggetti 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 GDPR (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);
g) trattati nella misura necessaria al perseguimento dei fini per i quali vengono raccolti (necessità).
3. L’Università adotta misure tecniche e organizzative adeguate in grado di comprovare il rispetto dei principi di cui al precedente comma (accountability) tenuto conto dello stato dell’arte, dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento,
4. Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale trovano applicazione le specifiche condizioni previste dagli artt. 44 e ss. del Regolamento (UE) 2016/679 affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dalla normativa europea**.**

ART. 4 - BASE GIURIDICA

1. L'Università è una pubblica amministrazione ai sensi dell'art. 1, c. 2 del d. lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. L'Università può trattare i dati personali quando ricorre una delle condizioni previste dall'art. 6, par. 1 e dall'art. 9, par. 2 del RGPD.

2. I trattamenti dei dati personali effettuati dall'Università per il perseguimento delle finalità istituzionali e dei compiti ad esse connesse trovano fondamento nella base giuridica prevista dall'art. 6, par. 1, lett. e) del RGPD.

2.1 Come previsto dall'art. 2-ter del d.lgs. 196/2003 e ss.mm.ii., la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di poteri pubblici è costituita da una norma di legge o di regolamento o da atti amministrativi generali.

2.2.In base al comma 1-bis dell'art. 2-ter del d.lgs. 196/2003 e ss.mm.ii., fermo restando ogni altro obbligo previsto dal RGPD e dal Codice privacy (nella versione aggiornata), il trattamento dei dati personali da parte di un'amministrazione pubblica è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad essa attribuiti.

PARTE II
CIRCOLAZIONE DEI DATI
ART. 5
CIRCOLAZIONE DEI DATI ALL'INTERNO DELL'UNIVERSITÀ

1.L'accesso ai dati personali da parte delle strutture amministrative, di servizio, didattiche e scientifiche e dei dipendenti dell'Università, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della libera circolazione delle informazioni all'interno dell'Ateneo, secondo il quale l'Università provvede all'organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico.

2.Ogni richiesta d'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, debitamente motivata e connessa con lo svolgimento dell'attività inerente alla loro specifica funzione, sarà soddisfatta in via diretta e senza ulteriori formalità nella misura necessaria- pertinente e non eccedente - al perseguimento dell'interesse istituzionale. Laddove invece la richiesta fosse finalizzata ad un utilizzo ulteriore e/o diverso dei dati, sarà necessario, da parte dei richiedenti, segnalarlo in maniera esplicita e formale nella richiesta, da valutare a cura del Responsabile della banca dati, e l'autorizzazione sarà concessa o negata a seconda che il fine della richiesta rientri o meno nell'attività istituzionale dell'Università.

3.Ai fini dell'accesso ai dati sono equiparati alle strutture dell'Università gli organismi con funzioni di controllo e di valutazione quali il Collegio dei Revisori, il Nucleo di Valutazione ed ogni altro organo a cui espresse disposizioni normative affidino detti compiti.

ART. 6

CIRCOLAZIONE, COMUNICAZIONE E DIFFUSIONE DEI DATI A SOGGETTI TERZI

1. La comunicazione di dati personali tra soggetti che effettuano il trattamento di dati, diversi da quelli particolari di cui agli artt. 9 e 10 del GDPR per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, è consentita unicamente se prevista da una norma di legge o, nei casi previsti dalla legge, da una norma di regolamento.
2. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del precedente comma 1.

3. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, degli studenti e neolaureati, l'Università potrà comunicare o diffondere, previa espressa richiesta o consenso del soggetto interessato, a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, e altri dati personali ad esclusione delle categorie dati di cui agli artt. 9 e 10 del GDPR, pertinenti in relazione alle predette finalità e ai compiti ad esse connesse.

4. Il trasferimento dei dati personali verso Paesi extra UE viene effettuato ai limiti e alle condizioni di cui agli artt. 44 e ss. del GDPR.

ART. 7
PUBBLICAZIONE DEI RISULTATI DI CONCORSI E SELEZIONI DEL PERSONALE DOCENTE E NON

1. In ottemperanza alla normativa vigente sulla trasparenza è consentita la pubblicazione, anche sui siti web di Ateneo, dei bandi di concorso per il reclutamento, a qualsiasi titolo, di personale docente e non, nonché i criteri di valutazione della Commissione, le tracce delle prove e le graduatorie finali con i nomi dei soli vincitori/idonei.
2. La pubblicazione degli atti sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati. La pubblicazione degli atti viene effettuata per il periodo di tempo previsto ai sensi di legge; decorso tale periodo gli atti sono rimossi dal sito web.
3. Non sono oggetto di pubblicazione informazioni relative allo stato di salute o alla situazione di disagio economico-sociale dei soggetti interessati.
4. Al fine di bilanciare l'esigenza di trasparenza con quella della protezione dei dati è consentita la pubblicazione della graduatoria con i nomi dei soli vincitori/idonei. I nomi delle persone inidonee o che non hanno superato la prova non devono essere pubblicati.

PARTE III
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO ED ORGANIGRAMMA PRIVACY

ART. 8
TITOLARE DEL TRATTAMENTO

Ai sensi della normativa vigente nazionale ed europea l'Università, in persona del Rettore pro-tempore, è titolare del trattamento dei dati personali.

1. Al Titolare del trattamento spettano le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali nonché agli strumenti utilizzati.
2. Il Titolare del trattamento, in virtù della normativa nazionale ed europea in materia di protezione dei dati personali, pone in essere gli adempimenti in materia di protezione dei dati e, in particolare, mette in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.
3. Il Titolare del trattamento, nell'ambito dei poteri che gli soni attribuiti dallo Statuto, può delegare il dirigente dell'Area presso cui è incardinato l'Ufficio Privacy alla firma degli atti relativi all'esercizio dei diritti dell'interessato di cui all'art. 25 del presente Regolamento.

ART. 9 RESPONSABILE DEL TRATTAMENTO

1. L'Università quando per la realizzazione delle proprie finalità istituzionali si avvale di un soggetto terzo per l'esecuzione di specifiche attività che comportano il trattamento di dati personali, il Titolare provvede a nominarlo Responsabile del trattamento ai sensi dell'art. 28 del GDPR.
2. Il Responsabile del trattamento viene individuato tra soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi la normativa in materia di protezione dei dati e garantisca la tutela dei diritti dei soggetti interessati.
3. La nomina del Responsabile viene effettuata tramite contratto o altro atto giuridico avente forma scritta, che individua la natura, le finalità e la durata del trattamento, il tipo di dati personali trattati e le categorie di soggetti interessati, definendo gli obblighi del Responsabile, nel rispetto delle previsioni di cui all'art. 28, par. 3, del GDPR.
4. Il Responsabile del trattamento può essere autorizzato a ricorrere ad un altro Responsabile (sub-Responsabile) per l'esecuzione di specifiche attività di trattamento purché siano imposti al sub-Responsabile i medesimi obblighi che gravano in capo al Responsabile. In ogni caso, il Responsabile del trattamento conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi da parte del sub-Responsabile.
5. L'Università può essere nominata Responsabile del trattamento quando effettua, in base a un contratto o altro atto giuridico avente forma scritta, trattamenti di dati personali per conto di un altro Titolare.

ART. 10
I SOGGETTI AUTORIZZATI AL TRATTAMENTO-INCARICATI DEL TRATTAMENTO

I soggetti Autorizzati al trattamento sono le persone fisiche istruite e formate dal Titolare a compiere, sotto la loro autorità e attenendosi alle istruzioni ricevute, operazioni di trattamento di dati.

1. Le persone fisiche che effettuano trattamenti di dati personali all'interno dell'Ateneo

sono:
a) il personale docente, ricercatori, il personale tecnico-amministrativo;
b) i collaboratori e le collaboratrici afferenti alle strutture amministrative e di servizio nonché di didattica e di ricerca;
c) i/le componenti degli organi centrali di Ateneo come definiti dall'art. 3 dello Statuto e degli altri organismi e comitati che operano in senso allo stesso;
d) tutti gli altri soggetti che trattano dati personali nell'ambito dell'organizzazione, quali a titolo esemplificativo e non esaustivo, studenti, dottorandi/e, assegnisti/e di ricerca, stagisti/e, tirocinanti (per tesi di laurea/dottorato, collaborazioni, attività di ricerca, attività di stage, tirocinio).

2. L'autorizzazione al trattamento dei dati personali può essere effettuata, anche in modalità informatizzata, con provvedimenti a carattere generale e/o con atti specifici, a seconda della tipologia del trattamento e della natura dei dati trattati. Potrà essere altresì effettuata tramite la documentata preposizione della persona fisica ad una struttura/ufficio per la quale è individuato, per iscritto, l'ambito del trattamento consentito ed autorizzato agli afferenti alla struttura/ufficio medesimo.
3. I soggetti Autorizzati al trattamento si impegnano a mantenere la riservatezza sulle informazioni e i dati di cui vengano a conoscenza e comunque a non comunicarli e/o diffonderli senza autorizzazione nonché a segnalare tempestivamente al Titolare qualsiasi violazione in materia di protezione dei dati personali.

ART. 11
RESPONSABILE PER LA PROTEZIONE DEI DATI- DATA PROTECTION OFFICER

1. L'Università, in quanto pubblica amministrazione, provvede ai sensi dell'art. 37, par. 1, lett. a) del GDPR alla designazione di un Responsabile della protezione dei dati (RPD).
2. Il RPD è individuato in base alle qualità professionali, alla conoscenza specialistica della normativa e della prassi europea e nazionale in materia di protezione dei dati nonché alla capacità di assolvere i compiti previsti dalla normativa.
3. Il RPD è tenuto a svolgere i seguenti compiti:
a) informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti ai collaboratori che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR e dalla normativa nazionale in materia di protezione dei dati.
b) assicurare l'osservanza del GDPR e di altre disposizioni derivanti dalla normativa comunitaria e nazionale, compresi l'attribuzione delle responsabilità e verificare la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
4. Il RPD redige una relazione annuale sull'attività svolta.

5. Al RPD sono garantite risorse adeguate e tempi di lavoro idonei allo svolgimento della sua funzione, anche avvalendosi di specifici gruppi di lavoro.

6. Il RPD ha accesso alle informazioni necessarie per svolgere i propri compiti ed è

interpellato/a per problematiche inerenti alla protezione dei dati e per attività che implicano un trattamento di dati fin dalla progettazione e per impostazione predefinita.
7.Il Titolare garantisce che il RPD eserciti le proprie funzioni in autonomia e indipendenza, impegnandosi altresì a non rimuoverlo e penalizzarlo a causa dell'adempimento dei propri compiti. In particolare, il RPD non può rivestire ruoli che lo/la portino a determinare mezzi e finalità del trattamento, né può rappresentare il Titolare o il Responsabile del trattamento.

ART. 12
TEAM PRIVACY E GRUPPO DI STUDIO PRIVACY

1. Il team Privacy, nominato con decreto del Rettore, è composto
- Dal delegato del Rettore alla Riservatezza/Privacy e in mancanza di un docente esperto della materia privacy
- Da un componente avente qualifica dirigenziale designato dal Direttore Generale
- Da un componente del personale tecnico amministrativo esperto in privacy.

2. Su richiesta del Team Privacy possono essere nominati referenti privacy nei singoli Dipartimenti.
3. Il team si riunisce periodicamente, e in ogni caso almeno una volta al mese, con il Responsabile per Protezione dei dati.
4. Il compito del Team privacy è quello di fornire supporto al Responsabile per la Protezione dei Dati (RPD- DPO): agevolare il raccordo tra il titolare del trattamento e il Responsabile per la Protezione dei dati.
5. Il team privacy, sempre di intesa con il RDP, propone e promuove attività di formazione e seminari rivolti al personale dell'Ateneo.
6. Il Rettore può nominare con proprio decreto, su richiesta del Team Privacy, un Gruppo di Studio PRIVACY. Il gruppo è presieduto dal delegato del Rettore competente (Delegato alla Privacy/Riservatezza) ed è composto da docenti in materie giuridiche, filosofiche e informatiche con comprovata esperienza in materia di privacy, protezione dei dati e sicurezza informatica. La funzione del gruppo - meramente di studio e consultiva - è quella di analizzare e migliorare le prassi relative alla protezione dei dati. Qualsiasi proposta del gruppo viene condivisa con il team privacy e il Responsabile per la protezione dei dati personali.

ART. 13
AMMINISTRATORI DI SISTEMA

1. Gli Amministratori di sistema sono i soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati e delle sue componenti, utilizzati in relazione ai trattamenti dei dati personali effettuati all'interno dell'Università di Foggia. Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e per la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali.
2. Ai fini del presente Regolamento, sono considerati Amministratori di sistema le figure professionali che operano nell'Università per l'amministrazione di basi di dati, di reti, di

apparati di sicurezza e di sistemi software complessi.
3. Il Titolare individua gli Amministratori di sistema con formale atto di designazione individuale, nel quale sono definiti in maniera analitica i compiti e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
4. Nel caso di notificazioni di violazioni di sicurezza dei dati, l'Amministratore di sistema notifica senza ritardo al titolare e al RPD eventuali anomalie riscontrate, malfunzionamenti o rischi di sicurezza.

5. L'Amministratore di sistema supporta gli Incaricati per gli aspetti di tipo tecnico-informatico nello svolgimento delle consuete attività operative istituzionali

PARTE IV LE TIPOLOGIE DI TRATTAMENTO
ART. 14
TRATTAMENTO DEI DATI PERSONALI

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 di interesse pubblico, come individuate da disposizioni di legge, statutarie e regolamentari e nel rispetto del GDPR, del Codice privacy nonché delle Linee guida e provvedimenti emanati dal Garante per la protezione dei dati personali.
2. L'Università effettua i trattamenti di dati personali, anche di natura particolare, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

a) la gestione del rapporto di lavoro del personale docente e della componente ricercatrice, del personale dirigente e tecnico–amministrativo, dei collaboratori e delle collaboratrici esterni/e, nonché dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato, ivi compresi i soggetti il cui rapporto di lavoro è cessato;
b) l'attività didattica e la gestione della carriera degli studenti intesi/e nell'accezione più ampia, ivi compresi laureati, dottorandi e tirocinanti;
c) l'attività di ricerca, compresa la ricerca in ambito medico, le attività didattiche e assistenziali connesse alla ricerca, le attività assistenziali effettuate nell'ambito delle strutture sanitarie convenzionate;
d) le attività gestionali e contrattuali, conto terzi e/o connessi ad attività trasversali, ivi compreso il trasferimento tecnologico.

ART. 15
CATEGORIE PARTICOLARI DI DATI

1. Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché quello di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (cd. Categorie particolari di dati) è vietato. Il trattamento può essere ammesso in presenza di una delle condizioni di seguito elencate (art. 9, comma 2, GDPR) :
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, nella misura in cui sia autorizzato dal diritto dell'Unione o nazionale o da un contratto collettivo, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale della persona interessata o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento riguarda dati personali resi manifestatamente pubblici dall'interessato;
e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
f) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o nazionale o conformemente al contratto con un professionista della sanità e i dati sono trattati da o sotto la responsabilità di un professionista soggetto a segreto professionale;
g) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, in conformità alle disposizioni dell'art. 89 del Regolamento UE;
h) il trattamento è necessario per motivi di interesse pubblico rilevante, se previsto dal diritto dell'Unione o dall'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili, e il motivo di interesse pubblico rilevante, nonché che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
2. Ai fini delle disposizioni di cui al precedente comma 1, lettera h), sono considerati di rilevante interesse pubblico i trattamenti eseguiti nelle materie previste dall'art. 2-sexies del Codice privacy.
3. I dati genetici, biometrici e relativi alla salute non possono essere diffusi e possono essere trattati solo in presenza di una delle condizioni di cui al comma 1 e in conformità alle misure di protezione disposte dal Garante privacy.

ART. 16
DATI RELATIVI A CONDANNE PENALI E REATI – DATI GIUDIZIARI

1. Il trattamento di dati personali relativi a condanne penali e a reati, oppure a connesse misure di sicurezza (dati c.d. giudiziari) è ammesso solo se autorizzato dal diritto dell'Unione o dall'ordinamento nazionale che preveda garanzie appropriate per i diritti e le libertà degli interessati.
2. Il trattamento dei dati di cui al comma 1 è ammesso, in particolare, nei seguenti casi, previsti dall'art. 2-octies del Codice privacy: a) adempimento di obblighi ed esercizio di diritti da parte del Titolare o dell'interessato nell'ambito dei rapporti di lavoro, nei limiti stabiliti da legge e regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9 e 88 del RGPD; b) adempimento di obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione di controversie civili e commerciali; c) verifica o accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti; d) accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nei limiti di quanto previsto dalle leggi o dai

regolamenti in materia; e) accertamento, esercizio o difesa di un diritto in sede giudiziaria; f) esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia; g) adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto; h) accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti; i) adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

ART. 17
TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DEL RAPPORTO DI LAVORO

1. L'Università tratta i dati personali del personale docente e della componente ricercatrice, del personale dirigente e tecnico–amministrativo e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato, adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi applicabili.
2. Il trattamento dei dati particolari relativi al personale se necessario può essere effettuato per motivi di interesse pubblico rilevante come definiti dall'art. 2 sexies del Codice privacy; 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; per accertare, esercitare o difendere un diritto in sede giudiziaria; a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità all'art. 89, par. 1, del GDPR (art. 9, par. 2, lett. g), b), f), j) del GDPR).
3. Il personale osserva le misure tecniche e organizzative indicate dall'Università per garantire la sicurezza del trattamento dei dati personali, anche da remoto o anche in modalità lavoro agile.
4. Il personale mantiene la riservatezza su tutti i dati personali trattati in ragione dello svolgimento della propria attività.

ART. 18
CARRIERE DEGLI STUDENTI E ATTIVITA' DIDATTICA

1. L'Università di Foggia tratta i dati personali degli studenti, intesi/e nella loro accezione più ampia, per lo svolgimento delle procedure di ammissione e di immatricolazione ai corsi di laurea, post-laurea e tirocini, e di tutte le attività relative alla gestione della carriera degli studenti.
2. Resta ferma la tutela del diritto dello studente alla riservatezza ai sensi dell'art. 2, comma 2, del DPR n. 249 del 24 giugno 1998.

ART. 19
TRATTAMENTO DEI DATI PER FINI DI RICERCA SCIENTIFICA, STORICA O A FINI STATISTICI.

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato da chiunque operi nell'ambito delle Strutture dell'Università garantendo il rispetto del principio della minimizzazione dei dati e dei principi sanciti nel GDPR e nel Codice Privacy (versione aggiornata).
2. Ove possibile e senza pregiudicare il raggiungimento delle finalità del trattamento, i

dati dovranno essere trattati con misure tecniche che non consentano più di identificare l'interessato.
3. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità secondo i principi stabiliti dall'articolo 5 del RGPD.
4. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.
5. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42, dalle relative regole deontologiche e dai Regolamenti di Ateneo in materia.
6. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto delle regole deontologiche in materia approvate dal Garante privacy.
7. Il trattamento di dati personali ai fini statistici o di ricerca scientifica da parte di chiunque operi all'interno di Uffici e Strutture dell'Università o per conto dell'Università stessa, deve avvenire nel rispetto dei seguenti principi: a) i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né trattati per altri scopi; b) all'interessato deve essere fornita puntuale informazione relativamente alle finalità statistiche o di ricerca scientifica del trattamento, a meno che questo non richieda uno sforzo sproporzionato rispetto al diritto tutelato e sempre che siano adottate le idonee forme di pubblicità individuate dalle regole deontologiche in materia, promosse dal Garante.

PARTE V
PROTEZIONE E SICUREZZA DEI DATI

ART. 20
REGISTRO DEL TRATTAMENTO

1. L'Università, in qualità di Titolare del trattamento, ha un Registro delle attività di trattamento svolte sotto la propria responsabilità e provvede al relativo aggiornamento.
2. Il Registro contiene le seguenti informazioni: a) la struttura competente in ordine al trattamento; b) ove esistenti, i nominativi e i dati di contatto del/i Contitolare/i e del/i Responsabile/i del trattamento; c) le finalità del trattamento; d) una descrizione delle categorie di interessati e delle categorie di dati personali; e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; f) l'eventuale trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, con l'indicazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate; g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; h) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.
3. Il registro dei trattamenti è unitario, ma ogni area/dipartimento provvede alla compilazione di propria competenza.
4. L'Università tiene altresì un Registro di tutte le categorie di trattamenti svolti in qualità di Responsabile per conto di altri Titolari di trattamento, contenente: a) la struttura competente in ordine al trattamento; b) il nominativo e i dati di contatto del Titolare per conto del quale l'Università agisce e del Responsabile della protezione dei dati; c) le

categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento; d) l'eventuale trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale, con l'indicazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate; e) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

ART. 21
FORMAZIONE DEL PERSONALE

1. Per garantire corretta e puntuale applicazione della disciplina in materia di protezione dei dati personali e della sicurezza informatica, l'Università sostiene e promuove, con il coinvolgimento degli organi istituzionali dell'Ateneo competenti per materia, strumenti di sensibilizzazione e attività formative finalizzati a consolidare la consapevolezza del valore della protezione dei dati personali e indirizzate al personale dell'Ateneo.

ART. 22
VALUTAZIONE DI IMPATTO

1. Quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie e considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università, prima di procedere al trattamento, effettua, consultandosi con il RPD, una valutazione dell'impatto sulla protezione dei dati personali. Può essere condotta una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Fatte salve le tipologie di trattamento individuate dal Garante, la valutazione d'impatto viene effettuata dall'Università nei seguenti casi: a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo significativamente analogo su dette persone; b) trattamento su larga scala di categorie particolari di dati personali di cui al precedente art. 17 o di dati relativi a condanne penali e a reati; c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico; d) trattamento di dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.
3. La valutazione di impatto contiene i seguenti elementi: a) una descrizione sistematica del trattamento e delle sue finalità; b) una valutazione in ordine alla necessità e alla proporzionalità del trattamento in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati; d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e in conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte.
4. Se necessario, l'Università procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto, quando insorgono variazioni del rischio rappresentato dalle attività di trattamento.

ART. 23 – MISURE TECNICHE ED ORGANIZZATIVE

1. L’Università in qualità di Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, misure che comprendono tra le altre la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L’Università adotta un approccio che tiene conto della protezione dei dati personali oggetto di trattamento sin dal momento della progettazione (by design) e per impostazione predefinita (by default) anche nella scelta e nella configurazione dei sistemi informativi e delle procedure operative.
4. Il Titolare, dopo l’entrata in vigore del presente Regolamento, può affidare il compito al gruppo di studio privacy - di intesa con DPO e team privacy e - di definire eventuali strategie, linee guida, policy.
5. I soggetti autorizzati sono istruiti e formati nell’osservare le misure tecniche e organizzative adeguate a limitare i rischi di distruzione o perdita, anche accidentale, e di accesso non autorizzato ai dati personali.

PARTE VI
DIRITTI DELL’INTERSSATO

ART. 24 ESERCIZIO DEI DIRITTI DELL’INTERESSATO

1.L’Università rispetta e riconosce i diritti dell’interessato di cui agli articoli da 15 a 22, secondo le specifiche modalità ivi previste.
2.In particolare, i diritti di:
a) accesso ai dati personali ovvero il diritto di conoscere e ottenere la conferma che sia in corso o meno
un trattamento dei dati personali e le informazioni ad esso relative;
b) rettifica, ovvero il diritto di correggere i dati personali inesatti, nonché di ottenere l’integrazione dei dati
incompleti senza ingiustificato ritardo;
c) cancellazione – «diritto all’oblio», ovvero il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nei casi in cui sia consentito dall’art. 17 del GDPR;
d) limitazione al trattamento, ovvero il diritto di impedire il trattamento dei dati personali che lo riguardano nelle ipotesi e alle condizioni previste dall’art. 18 del GDPR;
e) portabilità dei dati, ovvero il diritto a ricevere i dati conferiti al Titolare in un formato strutturato, di uso comune e leggibile meccanicamente e di trasmetterli ad altro Titolare nei soli casi in cui il trattamento sia basato sul consenso o su un contratto e sia effettuato con mezzi automatizzati;
f) opposizione al trattamento, ovvero il diritto di opporsi per motivi connessi alla sua condizione particolare a trattamenti per scopi di interesse pubblico o per legittimo interesse oppure a trattamenti per fini di ricerca scientifica, storica o a fini statistici, nonché per qualsiasi motivo a trattamenti per finalità di marketing;

g) revoca del consenso per i trattamenti effettuati sulla base del consenso stesso, in qualsiasi momento e con la stessa facilità con cui è stato accordato, senza pregiudicare la liceità dei trattamenti effettuati prima della revoca stessa.
2. L'esercizio dei diritti può essere esercitato dagli interessati senza formalità e in maniera gratuita. Tuttavia, saranno adottate tutte le misure ragionevoli per verificare previamente l'identità dell'interessato o di un/una suo/a delegato/a, quali la richiesta di documenti identificativi, atti di procura legale, atti di nomina del tutore o della tutrice, deleghe.
3. Sulla pagina del sito di Ateneo, nella sezione privacy, è indicato l'indirizzo email a cui inviare la richiesta. (https://www.unifg.it/it/privacy)
4. Il titolare del trattamento e gli uffici preposti, sentito il RPD, devono dare riscontro alla richiesta di esercizio dei diritti senza ingiustificato ritardo e comunque al più tardi entro un mese dal ricevimento della stessa. Tale termine potrà, tuttavia, essere prorogato per ulteriori due mesi in caso di particolare complessità della richiesta, anche in relazione alla mole dei dati richiesti, e al numero delle richieste effettuate, tenendo conto, in particolare dell'onere che comportano/della loro incidenza e onerosità rispetto al (tempo di) riscontro della richiesta.
5. A fronte di una richiesta manifestamente infondata o irragionevole, o qualora l'interessato fornisca informazioni false o ingannevoli al momento della presentazione della richiesta, il titolare del trattamento rifiuta la richiesta, motivandone il rigetto.
6. Resta in ogni caso salvo il diritto di proporre reclamo al Garante per la protezione dei dati ai sensi dell'art.77 del GDPR qualora l'interessato ritenga che il trattamento violi la normativa sulla protezione dei dati.
7. Si richiama la disposizione di cui all'art. 2 undecies Codice Privacy relativamente alla limitazione dei diritti dell'interessato. In particolare si ricorda che i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo

ART. 25
L'INFORMATIVA

1. Ogni struttura dell'Università assolve agli obblighi di informativa nei confronti dell'interessato ogniqualvolta provvede alla raccolta dei dati personali, informando l'interessato circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati richiesti;
b) la natura obbligatoria o facoltativa del conferimento di dati richiesti e le conseguenze di un eventuale rifiuto;
c) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
a. i diritti di cui al Codice;
b. il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare e, se designato, del responsabile.

2. L'informativa può essere resa per iscritto, nel modulo di iscrizione, in fogli presso le

strutture, o anche mediante informative di massa, come cartelli affissi nei locali in cui gli interessati si recano per conferire i dati (segreterie di Dipartimento, uffici del personale, ecc.) o mediante annunci sulle pagine Web.

3. Se i dati personali non sono raccolti presso l'interessato, l'informativa è data al medesimo all'atto della registrazione dei dati o non oltre la prima comunicazione, eccetto nei seguenti casi:

a) quando sono trattati in base ad un obbligo previsto dalla legge, da un Regolamento o dalla normativa comunitaria;
b) quando sono trattati per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati solo per tale finalità e per il periodo necessario al loro perseguimento;
c) quando l'informativa comporta un impiego di mezzi che il Garante ha dichiarato sproporzionato rispetto al diritto tutelato.

PARTE VII
SANZIONI E DATA BREACH
ART. 26 –VIOLAZIONE DEI DATI PERSONALI E SANZIONI

1. L'Università, con comunicazione del RPD, notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica al Garante non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. La notifica deve contenere i seguenti elementi: a) natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti; b) nome e dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni; c) probabili conseguenze della violazione dei dati personali; d) misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

3. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università comunica la violazione all'interessato senza ingiustificato ritardo.

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

5. Nel caso in cui l'Università non abbia comunicato all'interessato la violazione dei dati personali, il Garante, dopo aver valutato la probabilità che la violazione presenti un rischio elevato, può richiedere che vi si provveda o può decidere che una delle condizioni di cui al comma 5 risulti soddisfatta.

6. L'Università documenta qualsiasi violazione dei dati personali, le relative circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio.

6. Il Settore ICT supporta il Titolare coordinandosi con il RPD nella gestione del data breach.

9. Senza ingiustificato ritardo devono essere inviate via mail al Responsabile per la protezione dei dati tutte le informazioni relative al data breach.

PARTE VIII
MISCELLANEA

ART. 27 – VIDEOSORVEGLIANZA

1. Il trattamento dei dati realizzato mediante gli impianti di videosorveglianza collocati presso le sedi dell'Università è disciplinato dallo specifico Regolamento adottato dall'Ateneo in materia.

ART. 28 - DIRITTO DI ACCESSO E RISERVATEZZA

1. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela sono disciplinati dalla legge 7 agosto 1990, n. 241 e s.m.i. e dal Regolamento di disciplina del procedimento amministrativo, del diritto di accesso ai documenti amministrativi e del diritto di accesso civico adottato dall'Ateneo.
2. In caso di dati idonei a rivelare lo stato di salute o la vita sessuale, l'accesso ai documenti amministrativi è consentito quando la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi sia di rango almeno pari ai diritti dell'interessato evidenziati nel documento, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

DISPOSIZIONI FINALI

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

2. Le norme contenute in altri regolamenti universitari, in materia di protezione dei dati personali, confliggenti o incompatibili con il presente Regolamento, devono essere disapplicate.