



Università degli Studi “G. d’Annunzio”
Chieti - Pescara
Divisione I Affari Legali
Settore Normativa di Ateneo



REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

INDICE

PARTE GENERALE

- Art.1 - Ambito di applicazione
- Art.2 - Definizioni
- Art.3 - Tipologie di dati personali trattati dall’Università
- Art.4 - Principi generali del trattamento di dati personali
- Art.5 - Formazione, aggiornamento e cultura della consapevolezza
- Art.6 - Condizioni di liceità del trattamento di dati personali
- Art.7 - Circolazione di dati personali all’interno dell’Università

SOGGETTI DEL TRATTAMENTO DI DATI PERSONALI E PRINCIPIO DI RESPONSABILIZZAZIONE

- Art.8 - I soggetti del trattamento di dati personali
- Art.9 - Titolare del trattamento di dati personali
- Art.10 - Contitolare del trattamento di dati personali
- Art.11 - Autorizzati di I e di II livello e referenti del trattamento di dati personali
- Art.12 - Responsabile del trattamento
- Art.13 - Responsabile della protezione dei dati personali (DPO)
- Art.14 - Amministratori di sistema
- Art.15 - Ufficio *privacy* di Ateneo
- Art.16 - Comitato permanente di Ateneo per l’attuazione del Regolamento (UE) n. 679 del 2016
- Art.17 - Registri delle attività di trattamento
- Art.18 - Valutazione di impatto sulla protezione dei dati personali
- Art.19 - Consultazione preventiva
- Art.20 - Misure di sicurezza
- Art.21 - Violazione dei dati personali

TRASPARENZA E TUTELA DELL’INTERESSATO

- Art.22 - Informazioni all’interessato
- Art.23 - Diritti dell’interessato

TIPOLOGIE, OGGETTO DEI TRATTAMENTI E (LORO) FINALITÀ

- Art.24 - Trattamento di categorie particolari di dati personali
- Art.25 - Trattamento di dati relativi a condanne penali e reati
- Art.26 - Trattamento di dati personali nell’ambito del rapporto di lavoro
- Art.27 - Trattamento di dati personali in ambito sanitario
- Art.28 - Trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica
- Art.29 - Trattamento di dati personali a fini statistici o di ricerca scientifica
- Art.30 - Trattamento di dati personali a fini di ricerca medica, biomedica ed epidemiologica
- Art.31 - Trattamento di dati personali nelle sedute degli organi collegiali dei dati personali
- Art.32 - Comunicazione e diffusione

Art.33 - Trattamento di immagini

Art.34 - Videosorveglianza

NORME FINALI

Art.35 - Sanzioni

Art.36 - Entrata in vigore e rinvii

PARTE GENERALE

Art.1 - Ambito di applicazione

1. Il presente Regolamento, adottato in attuazione del Regolamento UE 27 aprile 2016 n.679 (di seguito, più semplicemente «Regolamento (UE) n. 679 del 2016») e del D. L.vo n.196/2003 come novellato dal D. L.vo n.101/2018 (di seguito, più semplicemente «Codice in materia di protezione dei dati personali» o «Codice»), disciplina la protezione delle persone fisiche in relazione al trattamento di dati personali effettuato dall’Università degli “Studi G. d’Annunzio” di Chieti-Pescara (di seguito, più semplicemente «Università» o «Ateneo»).

2. L’Università procede al trattamento di dati personali per lo svolgimento 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.

Art.2 - Definizioni

Ai fini del presente Regolamento si intende per:

1.«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, a titolo esemplificativo mediante il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2.«dato anonimo»: qualsiasi informazione non riferita a una persona fisica identificata o identificabile;

3.«categorie particolari di dati»: i dati personali che rivelino di una persona fisica (identificata o identificabile) l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale; i dati genetici; i dati biometrici; i dati relativi alla salute, alla vita sessuale e all’orientamento sessuale;

4.«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall’analisi di un campione biologico della persona fisica in questione;

5.«dati biometrici»: i dati personali ottenuti da un trattamento specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici;

6.«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

7.«interessato»: la persona fisica cui si riferiscono i dati personali;

8.«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;

9.«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo dei dati 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;

10.«processo decisionale automatizzato»: decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti nella sfera giuridica dell'interessato o che incide in modo analogo significativamente sullo stesso;

11.«pseudonimizzazione»: il trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;

12.«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

13.«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;

14.«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;

15.«responsabile della protezione dei dati personali» (di seguito, più semplicemente «D.P.O.»): la persona fisica designata dal titolare del trattamento per assolvere a funzioni di supporto, controllo, consultive e formative relativamente all'adeguamento delle attività di trattamento di dati personali al Regolamento (UE) n.679 del 2016, al Codice in materia di protezione dei dati personali e ai provvedimenti su tematiche specifiche adottati dal Garante per la Protezione dei Dati Personali;

16.«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;

17.«autorizzato al trattamento»: la persona fisica formalmente autorizzata e istruita a trattare i dati personali sotto la diretta autorità del titolare e/o del responsabile del trattamento;

18.«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. Non sono considerate destinatari le autorità pubbliche che ricevono comunicazioni di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri;

19.«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo diversi dall'interessato, dal titolare del trattamento, dal responsabile del trattamento e dagli autorizzati al trattamento;

20.«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

21.«comunicazione»: il dare conoscenza a uno o più soggetti determinati, dei dati personali, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o interconnessione, come ad esempio: la comunicazione di dati personali raccolti dall'Università ad altro soggetto pubblico;

22.«diffusione»: il dare conoscenza dei dati personali a soggetti indeterminati (diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dai responsabili e dai soggetti autorizzati al trattamento) in qualunque forma, anche mediante la loro messa a disposizione o consultazione, come ad esempio la pubblicazione di dati personali sul sito istituzionale dell'Università;

23.«registro delle attività di trattamento»: l'elenco dei trattamenti di dati in forma cartacea o telematica effettuati dal titolare e/o dal responsabile del trattamento secondo i rispettivi ambiti del trattamento;

24.«valutazione d'impatto sulla protezione dei dati»: la procedura atta a descrivere il trattamento, a valutarne la necessità e proporzionalità e a garantire la gestione dei rischi per i diritti e le libertà degli interessati;

25.«violazione dei dati personali»: la violazione 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;

26.«autorità di controllo»: l'autorità pubblica indipendente, istituita da uno Stato membro ai sensi dell'art.51 del Regolamento UE 679 del 2016, incaricata di sorvegliare l'applicazione del Regolamento stesso, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (per l'Italia, l'Autorità di Controllo è individuata dal Codice (art. 153 e segg.) nel Garante per la Protezione dei Dati Personali);

27.«amministratori di sistema»: la figura professionale dedicata alla gestione e alla manutenzione degli impianti di elaborazione o di sue componenti, compresi gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi.

Art.3 - Tipologie di dati personali trattati dall'Università

1.L'Università è un'istituzione di alta cultura, con personalità giuridica di diritto pubblico, che ha come proprio fine istituzionale la ricerca scientifica e la formazione, ritenute tra loro inscindibilmente legate, nonché, per i corsi di laurea che la contemplano, l'assistenza sanitaria. L'Ateneo promuove lo sviluppo e la diffusione delle conoscenze e del sapere scientifico, per favorire il progresso culturale, civile ed economico della società, anche nella prospettiva dell'interazione tra le culture e della generazione di *spinoff*.

2.Per il perseguimento dei propri fini istituzionali l'Università tratta principalmente le tipologie di dati personali qui di seguito indicate.

a) Dati personali, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, compresi i soggetti di cui il rapporto di lavoro è cessato, o altro personale operante a vario titolo nell'Università quali, in via meramente esemplificativa e non tassativa, borsisti e tirocinanti. Tali dati vengono trattati nell'ambito delle seguenti attività:

- prove concorsuali/selezioni;
- gestione del rapporto di lavoro;
- formazione e aggiornamento professionale;
- gestione di progetti di ricerca;
- monitoraggio e valutazione della ricerca;
- valutazione della *performance*;
- attività di trasferimento tecnologico;
- attività di *welfare*;
- salute e sicurezza delle persone nei luoghi di lavoro;
- accesso ad aree riservate e parcheggi di pertinenza dell'Università;
- *smart working* e telelavoro;
- erogazione del servizio di telefonia fissa e *mobile*;
- erogazione del servizio di posta elettronica e di posta elettronica certificata;
- procedimenti di natura disciplinare a carico del personale.

b) Dati personali, 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 e verifica dei requisiti di accesso;
- erogazione del percorso formativo e gestione della carriera (dall'immatricolazione al conseguimento del titolo);
- erogazione di attività didattica ed esami in modalità remota;
- attività di tirocinio e stage;
- attività di orientamento;
- attività di *job placement*;
- attività connesse allo svolgimento delle elezioni studentesche e alla rappresentanza degli studenti negli organi di governo dell'Ateneo;
- attività connesse alle associazioni di ex-alunni;
- attività di *fundraising*, di comunicazione e informazione istituzionale e sviluppo di *community*;
- rilevazioni statistiche;

- valutazione delle attività didattiche;
 - riscontro a richieste inoltrate dall’Autorità Giudiziaria, dalle Forze dell’Ordine o da altre pubbliche amministrazioni;
 - servizi di tutorato, assistenza, inclusione sociale;
 - servizi di assistenza ai disabili e DSA;
 - servizi e attività per il diritto allo studio;
 - procedimenti disciplinari a carico di studenti.
- c) Dati personali relativi alla didattica e alla ricerca (compresa la ricerca in ambito medico-sanitario).
- d) Dati personali relativi alle attività gestionali interne all’Ateneo e alle attività svolte per conto di soggetti terzi. Tali dati vengono trattati nell’ambito delle seguenti attività:
- gestione degli spazi;
 - gestione delle postazioni;
 - gestione degli organi e delle cariche istituzionali;
 - gestione degli infortuni;
 - servizi bibliotecari;
 - servizi di protocollo e di conservazione documentale;
 - acquisto di beni e servizi, stipulazione di contratti, recupero crediti, gestione del contenzioso;
 - servizi di posta elettronica;
 - servizi di didattica e di svolgimento degli esami in modalità remota;
 - tracciamento di informazioni per finalità connesse alla sicurezza dei sistemi informatici;
 - svolgimento di prove di accesso e procedure concorsuali.

3. Si intendono comunque disciplinati dal presente Regolamento tutti i trattamenti di dati personali, anche di natura particolare, svolti dall’Università, anche se non presenti nei succitati elenchi, che siano strumentali al perseguimento dei suoi fini istituzionali e, più in generale, dei compiti assegnategli dalla legge.

Art.4 - Principi generali del trattamento di dati personali

1. Il trattamento dei dati personali viene effettuato dall’Università nel rispetto dei principi generali sanciti dall’art. 5 del Regolamento (UE) n. 679 del 2016.

2. I dati personali oggetto di trattamento sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell’interessato;
- 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’art. 89, par. 1 del Regolamento (UE) n. 679 del 2016, considerato incompatibile con le finalità originarie del trattamento;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati;
- 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’art. 89, par. 1 del Regolamento (UE) n. 679 del 2016;
- 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 anche meramente accidentali.

3. Valutati la natura, l’oggetto, il contesto, le finalità e gli (eventuali) rischi del trattamento, l’Università adotta misure tecniche e organizzative adeguate, in grado di garantire, documentare e comprovare il rispetto dei principi sopra enunciati.

4. Fatto salvo quanto previsto dai precedenti commi, i sistemi forniti e i servizi erogati dall’Università sono configurati in modo tale da ridurre al minimo il trattamento di dati personali.

5. 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) n. 679 del 2016, affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dalla normativa europea.

Art.5 - Formazione, aggiornamento e cultura della consapevolezza

1. Al fine di garantire, nell’esercizio delle attività istituzionali, la corretta applicazione della normativa in materia di protezione dei dati personali, oltre che, più in generale, la diffusione di una cultura della consapevolezza sul tema della protezione dei dati, l’Università promuove, con il coinvolgimento del D.P.O. e degli altri organi e/o uffici competenti per materia, periodiche attività di formazione indirizzate al personale dell’Ateneo.
2. L’Università predispone ogni anno, sentito il D.P.O., un piano formativo in materia di trattamento di dati personali e di prevenzione dei rischi di violazione. Tale piano formativo è integrato e coordinato con le attività di formazione in materia di prevenzione della corruzione, nonché in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l’Università.
3. La frequenza alle attività di formazione è obbligatoria.

Art.6 - Condizioni di liceità del trattamento di dati personali

1. Il trattamento di dati personali, anche di natura particolare, è lecito nella misura in cui ricorra almeno una delle seguenti condizioni:
- il trattamento dei dati è necessario all’esecuzione dei compiti di interesse pubblico e connessi all’esercizio dei pubblici poteri attribuiti all’Università da norme di legge o di regolamento;
 - il trattamento dei dati è necessario all’adempimento di obblighi contrattuali di cui l’interessato è parte o all’esecuzione di misure precontrattuali adottate su richiesta dello stesso;
 - il trattamento dei dati è necessario all’adempimento di obblighi di legge cui è soggetta l’Università;
 - il trattamento dei dati è necessario al perseguimento del legittimo interesse dell’Università, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell’interessato;
 - il consenso dell’interessato, ove previsto.

Art.7 - Circolazione di dati personali all’interno dell’università

1. L’accesso ai dati personali da parte delle strutture amministrative, di servizio, didattiche e scientifiche e da parte dei dipendenti e/o collaboratori dell’Università, comunque limitato ai casi in cui sia strumentale al perseguimento delle finalità istituzionali dell’Ateneo, è ispirato al principio della libera circolazione delle informazioni all’interno dell’Ateneo medesimo, secondo il quale l’Università provvede all’organizzazione delle informazioni e dei dati a propria disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l’accesso e la fruizione.
2. L’accesso ai dati personali è consentito in via diretta e senza ulteriori formalità, nella misura necessaria al perseguimento delle finalità istituzionale dell’Università, ferma restando la responsabilità del richiedente derivante dall’eventuale utilizzo illecito, non necessario, non pertinente o comunque improprio dei dati, cui questi ha avuto accesso.

SOGGETTI DEL TRATTAMENTO DI DATI PERSONALI E PRINCIPIO DI RESPONSABILIZZAZIONE

Art.8 - I soggetti del trattamento di dati personali

- Nel trattamento di dati personali per i fini istituzionali dell’Università, le figure di riferimento sono le seguenti:
- il titolare del trattamento;

- i responsabili del trattamento;
- il responsabile della protezione dei dati personali (D.P.O.);
- gli autorizzati al trattamento di I e di II livello;
- gli amministratori di sistema.

Art.9 - Titolare del trattamento di dati personali

1. Il titolare del trattamento dei dati personali effettuato nell’esercizio delle (sue) attività istituzionali è l’Università G. d’Annunzio, con sede legale a Chieti, in Via Vestini 31, legalmente rappresentata dal Magnifico Rettore.

2. Al titolare del trattamento spettano le decisioni in ordine alle finalità e alle modalità del trattamento dei dati personali nonché agli strumenti utilizzati.

3. Il titolare del trattamento è tenuto a dare attuazione agli adempimenti imposti dalla normativa in materia di protezione dei dati e, in particolare, (ad) adottare misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

4. Al fine di garantire l’attuazione della normativa in materia di protezione dei dati personali, il titolare del trattamento si avvale di soggetti che operano sotto la sua diretta autorità, designati quali autorizzati al trattamento dei dati personali, nonché di soggetti esterni, designati quali responsabili del trattamento.

Art.10 - Contitolare del trattamento di dati personali

1. L’Università è contitolare quando con uno o più titolari del trattamento determina congiuntamente le finalità

e i mezzi del trattamento.

2. Nel caso in cui l’Università sia contitolare del trattamento con uno o più soggetti giuridici, mediante uno specifico accordo sono stabilite, in modo trasparente, le rispettive responsabilità in merito all’osservanza degli obblighi derivanti dal Regolamento (UE) n. 679 del 2016, con particolare riguardo all’esercizio dei diritti dell’interessato, oltre che le rispettive funzioni di comunicazione delle informazioni all’interessato, secondo quanto previsto dagli artt. 13 e 14 del citato Regolamento (UE).

3. Sulla base di quanto previsto dal precedente comma, l’interessato può esercitare i diritti riconosciutigli dal Regolamento (UE) n. 679 del 2016 nei confronti di (e contro) ciascun contitolare del trattamento.

Art.11 - Autorizzati di I e di II livello e referenti del trattamento di dati personali

1. Il titolare del trattamento provvede alla designazione degli autorizzati di I livello, individuandoli nei responsabili apicali di struttura, i quali hanno il compito di vigilare, monitorare e garantire, all’interno della struttura cui sono preposti, il rispetto della normativa vigente in materia di protezione dei dati personali, del presente regolamento e delle istruzioni fornite dal titolare medesimo.

2. Gli autorizzati di I livello possono designare, all’interno della propria struttura, un referente che avrà il compito di fungere da punto di contatto con il responsabile della protezione dei dati personali (v. successivo art. 12) per ogni necessità legata alle attività di trattamento di dati personali, oltre che collaborare attivamente e supportare il designante nella gestione delle attività relative al trattamento di dati personali.

3. I referenti sono individuati nell’ambito del personale tecnico-amministrativo in considerazione delle specifiche competenze richieste. All’interno dei Dipartimenti, i referenti possono essere individuati anche tra il personale docente, anche in questo caso considerando le specifiche competenze richieste.

4. I nominativi degli eventuali referenti devono essere comunicati al titolare del trattamento e al responsabile della protezione dei dati personali, tramite l’ufficio privacy di Ateneo.

5. Il titolare del trattamento (o, nell’ambito della propria struttura, l’autorizzato di I livello) provvede alla designazione degli autorizzati di II livello, individuandoli nelle persone fisiche che, appartenenti al personale tecnico-amministrativo o al personale docente, o che collaborano a vario titolo con l’Università, sono chiamate in ragione delle loro funzioni a trattare i dati personali di cui è titolare l’Università.

6. Gli autorizzati di II livello, nel trattare i dati personali di cui è titolare l'Università, sono tenuti al rispetto delle istruzioni impartite dal titolare del trattamento, dagli autorizzati di I livello, oltre che più in generale al rispetto della normativa vigente in materia di protezione dei dati personali e del presente regolamento. Sono tenuti a trattare i dati personali solo per le finalità per le quali sono stati autorizzati e per il tempo necessario. Sono tenuti a mantenere il massimo riserbo sui compiti perseguiti e a non comunicare a terzi notizie, informazioni o dati di cui siano venuti a conoscenza nella propria qualità di autorizzati. Sono tenuti a segnalare tempestivamente all'Ufficio Privacy d'Ateneo e al D.P.O. eventuali anomalie, incidenti, furti, perdite accidentali di dati, informando il proprio referente o, in mancanza, l'autorizzato di I livello. Sono tenuti altresì ad aggiornarsi costantemente sulle eventuali modifiche ed integrazione al dato normativo vigente e, conseguentemente, a partecipare attivamente alle iniziative di carattere formativo organizzate sul tema dall'Università.

Art.12 - Responsabile del trattamento

1. Il Responsabile del trattamento è il soggetto esterno all'organizzazione dell'Università che esegue trattamenti per conto dell'Università stessa. L'Università, in qualità di titolare del trattamento dei dati personali, designa quali responsabili del trattamento solo persone fisiche o giuridiche che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti sanciti dal Regolamento (UE) n. 679 del 2016 e garantisca la tutela dei diritti dell'interessato.

2. L'Università designa il responsabile del trattamento mediante un contratto o altro atto giuridico, anche in formato elettronico, che determina la natura, la durata e la finalità del trattamento o dei trattamenti assegnati, il tipo di dati trattati, le categorie di interessati, gli obblighi e i diritti del titolare, le istruzioni del titolare del trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare del trattamento e, più in generale, il rispetto della normativa vigente, le responsabilità derivanti dalla mancata osservanza dei compiti assegnati al responsabile e degli obblighi in capo a questo.

3. Gli obblighi specifici comunque imposti in capo al Responsabile del trattamento sono:

- il rispetto delle istruzioni fornite dal titolare del trattamento;
- la tenuta del registro dei trattamenti svolti per conto del titolare del trattamento;
- l'adozione di tutte le misure tecniche e organizzative idonee a garantire la sicurezza dei trattamenti e la tutela dell'interessato;
- la designazione di un responsabile della protezione dei dati (D.P.O.), se prevista dalla legge o se ritenuta necessaria in ragione della natura dei dati trattati, delle finalità del trattamento o dei rischi per la tutela dei diritti dell'interessato;
- la designazione di un rappresentante in Italia (nel caso di responsabile non stabilito nella UE);
- l'assistenza al titolare del trattamento, con misure tecniche ed organizzative adeguate, al fine di fornire riscontro alle richieste di esercizio dei diritti dell'interessato, oltre che al fine di fornire riscontro alle richieste di esercizio dei diritti dell'interessato, alle richieste dell'autorità di controllo e/o dell'autorità giudiziaria;
- garantire, su richiesta del titolare del trattamento, la cancellazione di tutti i dati personali al termine della prestazione di servizi relativi al trattamento o la loro restituzione al titolare del trattamento e la successiva cancellazione delle copie esistenti;
- la messa a disposizione a favore del titolare del trattamento di tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui al presente articolo e di quelli ulteriori al cui adempimento è tenuto per legge, consentendo al titolare del trattamento o da altro soggetto da questi incaricato lo svolgimento delle attività di revisione, controllo ed ispezione.

4. Il contratto o, più in generale, l'atto di designazione del responsabile può prevedere la possibilità che questi nomini sub-responsabili del trattamento esclusivamente previa autorizzazione scritta del titolare del trattamento. Eventuali sub-responsabili saranno sottoposti ai medesimi obblighi posti in capo al responsabile del trattamento. Il responsabile del trattamento, tuttavia, risponde della scelta effettuata ed

è tenuto a vigilare sull’operato del sub-responsabile. Qualora un sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile conserva nei confronti del titolare del trattamento l’intera responsabilità derivante dal mancato adempimento degli obblighi sanciti dalla legge, assumendo le conseguenze contrattuali e quelle extracontrattuali.

Art.13 - Responsabile della protezione dei dati personali (D.P.O.)

1. L’Università designa un Responsabile della Protezione dei Dati (di seguito, più semplicemente D.P.O.), soggetto di supporto al titolare del trattamento, con funzioni di raccordo con il Garante per la Protezione dei Dati Personali.

2. Il D.P.O. è designato in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa sulla protezione dei dati personali e delle prassi in materia di protezione dei dati, oltre che della capacità di assolvere ai propri compiti. Il D.P.O. è nominato con decreto del Rettore.

3. Il D.P.O. può essere un soggetto interno all’Università o un soggetto esterno con incarico affidato sulla base di un contratto di servizi. L’incarico ha durata triennale e può essere rinnovato.

4. Il D.P.O. svolge i seguenti compiti:

- informare e fornire consulenza al titolare del trattamento, ai responsabili del trattamento, agli autorizzati di I e II livello, organizzando, fra l’altro, incontri di formazione e aggiornamento professionale;
- sorvegliare l’osservanza della normativa vigente in materia di protezione dei dati personali, oltre che del presente regolamento e attivarsi tempestivamente all’accertamento di anomalie, criticità e violazioni;
- fornire, se richiesto, un parere in merito alla valutazione d’impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell’art. 35 del Regolamento (UE) n. 679 del 2016;
- cooperare con il Garante per la Protezione dei Dati Personali;
- fungere da punto di contatto tra l’Università, in qualità di titolare del trattamento e il Garante per la Protezione dei Dati Personali per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all’art. 36 del Regolamento (UE) n. 679 del 2016, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- collaborare alla predisposizione e all’aggiornamento dei registri del trattamento;
- collaborare con l’Ufficio privacy di Ateneo (v. successivo art. 15);
- svolgere ogni ulteriore compito attribuitogli dall’Università, se compatibile con le sue funzioni e il suo ruolo.

5. Nello svolgimento dei propri compiti, il D.P.O. considera debitamente i rischi sottesi ai trattamenti di dati personali di cui è titolare l’Università, tenuto conto della natura, dell’ambito di applicazione, del contesto e delle finalità dei trattamenti, oltre che della natura dei dati trattati.

6. Al D.P.O. sono garantite le risorse necessarie per assolvere i propri compiti, accedere ai dati personali e alle operazioni di trattamento su di essi effettuati, e per mantenere la propria conoscenza specialistica.

7. Il D.P.O. deve essere coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

8. L’Università garantisce che il D.P.O. eserciti le proprie funzioni in autonomia e indipendenza.

9. Il D.P.O. è tenuto a redigere annualmente la relazione sull’attività svolta e sullo stato di attuazione in Ateneo della normativa sulla protezione dei dati personali. La relazione annuale è trasmessa al Rettore, al Senato accademico e al Consiglio di amministrazione.

10. Il nominativo e i dati di contatto del D.P.O. sono inseriti nelle informative sul trattamento dei dati personali e sono pubblicati sul sito istituzionale dell’Università.

Art. 14 - AMMINISTRATORI DI SISTEMA

1. Secondo quanto previsto dal provvedimento del Garante del 27 novembre 2008, sono amministratori di sistema 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.

2. Gli amministratori di sistema sviluppano e gestiscono l'impianto di elaborazione o i suoi componenti *hardware* e *software* tramite i quali vengono effettuati i trattamenti di dati personali, applicando per i profili relativi alla sicurezza le istruzioni impartite dal titolare e, più in generale, adottando tutte le misure tecniche ed organizzative richieste dalla normativa vigente.

3. Gli amministratori di sistema sono designati dal Rettore con atto scritto che definisce analiticamente i compiti e gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Art.15 - Ufficio Privacy di Ateneo

1. L'Università, al fine di armonizzare le procedure organizzative sottese al trattamento dei dati personali effettuato nello svolgimento delle sue finalità istituzionali, ha predisposto uno specifico ufficio privacy di Ateneo.

2. L'ufficio privacy di Ateneo, articolazione del Settore Anticorruzione, Trasparenza e Privacy, ha le seguenti funzioni:

- attività di supporto alle strutture ed articolazioni dell'Università per il trattamento dei dati personali, al fine di garantire un'uniforme, efficace e completa applicazione della normativa vigente e la sua conseguente osservanza;
- attività di supporto al D.P.O. per il corretto espletamento delle sue prerogative ed in particolare delle attività di controllo e di vigilanza sul trattamento dei dati personali effettuato dall'Università nell'esercizio delle sue funzioni istituzionali;
- attività di predisposizione di modelli documentali (ad esempio, informative sul trattamento dei dati personali);
- attività di tenuta del registro dei *data breach* e delle segnalazioni pervenute dagli interessati;
- attività di diffusione di una cultura della consapevolezza, organizzando gli incontri di formazione e aggiornamento, destinati al personale dell'Università, secondo quanto previsto dal precedente art. 5;
- attività di supporto al personale amministrativo e docente, al fine di chiarire dubbi e risolvere problematiche attinenti alla corretta applicazione della normativa vigente.

Art.16 - Comitato permanente di ateneo per l'attuazione del regolamento (UE) n.679 del 2016

1. L'Università, al fine di coordinare le attività necessarie all'adeguamento delle operazioni di trattamento dei dati personali alla normativa vigente, anche in considerazione di un assetto normativo in costante evoluzione, ha designato un comitato permanente di ateneo per l'attuazione del Regolamento (UE) n. 679 del 2016.

2. Il comitato, composto da membri del personale amministrativo, oltre che da docenti dell'Ateneo, scelti in ragione delle competenze specialistiche sulla materia della protezione dei dati personali, uno dei quali è designato Coordinatore, è nominato con decreto dal Rettore.

3. Il comitato ha le seguenti funzioni:

- attività di supporto, in funzione propositiva e consultiva, all'attuazione degli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali;
- attività di predisposizione, ove necessario, di linee guida e *policy* d'uso, strumentali a fornire indicazioni operative nel trattamento dei dati personali strumentale all'espletamento delle funzioni istituzionali dell'Ateneo;
- attività di supporto all'Ufficio privacy di Ateneo nell'attività di diffusione di una cultura della consapevolezza, rendendosi disponibile, in ragione delle competenze dei suoi componenti, all'attività di docenza nei corsi di formazione e aggiornamento che l'Ateneo organizza periodicamente;
- attività di supporto al D.P.O. e all'ufficio privacy, tramite attività di indirizzo e, ove necessario, consulenza.

4. Alle riunioni periodiche del comitato partecipa il D.P.O.

Art. 17 – I REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

1. L'Università, in qualità di titolare del trattamento, istituisce i registri delle attività di trattamento dei dati effettuate nell'espletamento delle proprie finalità istituzionali. I registri censiscono le attività di

trattamento svolte dagli uffici e dalle strutture dell’Università e le principali caratteristiche dei trattamenti. I registri, tenuti in forma scritta, anche in formato elettronico, sono costantemente aggiornati e, su richiesta, messi a disposizione del Garante per la protezione dei dati personali.

2. I registri contengono le seguenti informazioni:

- la struttura competente in ordine al trattamento;
- ove esistenti, i nominativi e i dati di contatto del/i contitolare/i e del/i responsabile/i del trattamento;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali oggetto di trattamento;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- 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;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

2. Per consentire la tenuta del registro, nel caso di inizio o cessazione di un trattamento, il responsabile della struttura interessata, anche tramite il referente eventualmente individuato, informa tempestivamente il titolare, l’Ufficio Privacy d’Ateneo e il D.P.O. fornendo tutte le informazioni utili all’inserimento del trattamento nel registro tenuto nella struttura.

3. L’Università, se del caso, tiene altresì un registro di tutte le categorie di trattamenti svolti in qualità di responsabile per conto di altri titolari di trattamento, contenente le seguenti informazioni: la struttura competente in ordine al trattamento; il nominativo e i dati di contatto del titolare per conto del quale l’Università agisce e del D.P.O.; le categorie dei trattamenti effettuati dall’Università per conto del titolare del trattamento; 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; ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Art. 18 - VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

1. Nell’ipotesi in cui un trattamento di dati personali, prevedendo l’uso di nuove tecnologie, considerati la natura, l’oggetto, il contesto e le finalità del trattamento medesimo, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l’Università effettua, consultandosi con il D.P.O., una preliminare valutazione dell’impatto sulla protezione dei dati personali. Coerentemente al disposto dell’art. 35 del Regolamento (UE) n. 679 del 2016, può essere condotta una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. La valutazione di impatto viene effettuata dall’Università nei casi in cui il trattamento di dati personali, ancorché strumentale al perseguimento delle finalità istituzionali dell’Ateneo, possa comportare:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo significativamente analogo su dette persone;
- un trattamento su larga scala delle categorie particolari di dati personali di cui all’art. 9 del Regolamento (UE) n. 679 del 2016 o di dati relativi a condanne penali e a reati;
- una sorveglianza, di carattere sistematico e su larga scala, di una zona accessibile al pubblico;
- un 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

- una descrizione sistematica del trattamento e delle sue finalità;
- una valutazione in ordine alla necessità e alla proporzionalità del trattamento in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;

- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento (UE) n. 679 del 2016, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte.

4. Successivamente alla valutazione di impatto, l'Università può procedere ad un riesame finalizzato a valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione di impatto medesima.

5. Gli autorizzati di I livello devono comunicare, anche per il tramite dell'Ufficio Privacy di Ateneo, al titolare tutti i nuovi trattamenti che intendono effettuare, per consentire allo stesso di effettuare, ove necessario, la valutazione di impatto.

6. L'Università qualifica, coerentemente alle indicazioni del Garante per la protezione dei dati personali e delle Linee Guida del Gruppo Art. 29, la valutazione di impatto una buona prassi da effettuarsi, oltre che nelle specifiche ipotesi di cui al precedente comma 2°, ogniqualvolta se ne ravvisi, anche per il tramite del confronto con il D.P.O., l'opportunità, in ragione delle caratteristiche del trattamento di dati personali che si intende effettuare.

7. Qualora, a seguito della valutazione di impatto, risulti che il trattamento dei dati personali potrebbe comportare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Università deve consultare il Garante per la protezione dei dati personali nel rispetto di quanto previsto dal successivo art. 19.

ART. 19 - CONSULTAZIONE PREVENTIVA

1. L'Università consulta il Garante per la protezione dei dati personali, ai sensi del precedente art. 18, ult. comma., per il tramite del D.P.O.

2. In sede di consultazione, l'Università comunica al Garante per la protezione dei dati personali:

- le rispettive responsabilità dell'Università in qualità di titolare del trattamento, nonché di eventuali contitolari e dei responsabili del trattamento;
- le finalità e i mezzi del trattamento;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
- i dati di contatto del D.P.O.;
- la valutazione di impatto sulla protezione dei dati;
- ogni altra informazione richiesta dal Garante per la protezione dei dati personali.

3. Se il Garante ritiene che il trattamento di dati personali previsto violi il Regolamento (UE) n. 679 del 2016, in particolare allorché l'Università non abbia identificato o attenuato sufficientemente il rischio, l'Autorità fornisce, entro un termine di otto settimane, decorrenti dal ricevimento della richiesta di consultazione, un parere scritto all'Università. Tale periodo può, coerentemente a quanto previsto dall'art. 36 del Regolamento (UE) n. 679 del 2016, essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. Il Garante informa l'Università di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.

ART. 20 - LE MISURE DI SICUREZZA

1. Tenendo conto dello stato dell'arte, 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, l'Università adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio. Nel valutare l'adeguato livello di sicurezza, l'Università considera in particolare le conseguenze derivanti 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.

2. 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.

3. L'Università definisce le misure tecniche e organizzative, anche tramite specifiche linee guida, cui dovranno attenersi scrupolosamente tutti i responsabili del trattamento e gli autorizzati di I e II livello, fermo restando l'obbligo di osservare le istruzioni di sicurezza già indicate nei rispettivi atti di designazione.

4. Specifiche misure di sicurezza, tecniche ed organizzative, ulteriori rispetto a quelle individuate dall’Università, potranno essere adottate dagli autorizzati di I livello (o, se presenti, dai referenti del trattamento dei dati personali), qualora risultino necessarie in relazione a specifiche esigenze della struttura gestita, tenuto conto del livello di esposizione al rischio individuato per le peculiari attività di trattamento effettuate.

6. Gli autorizzati di I livello si coordinano con il D.P.O. nell’esecuzione dell’analisi dei rischi e dell’eventuale valutazione di impatto, adottando metodologie riconosciute a livello nazionale e internazionale.

7. L’Università monitora, anche per il tramite del D.P.O. e degli autorizzati di I livello (e, se presenti, dei referenti del trattamento dei dati), l’applicazione delle misure di sicurezza tecniche e organizzative all’interno dell’Ateneo e presso i soggetti designati responsabili del trattamento, adottando se del caso i necessari provvedimenti.

Art. 21 - VIOLAZIONE DEI DATI PERSONALI

1. In caso di violazione dei dati personali, l’Università, con il supporto del D.P.O., notifica la violazione al Garante per la protezione dei dati personali, 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. Le notifiche effettuate oltre il termine delle 72 ore devono essere accompagnate dall’enunciazione dei motivi del ritardo.

2. La notifica deve contenere almeno i seguenti elementi:

- la descrizione della 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 nella violazione;
- il nome e i dati di contatto del D.P.O. o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l’adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

3. Qualora e nella misura in cui non sia possibile fornire le succitate informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

4. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l’Università comunica la violazione all’interessato senza ingiustificato ritardo. La comunicazione all’interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni, di cui al precedente comma 2, già enunciate nella notifica al Garante per la protezione dei dati personali.

5. Non è richiesta la comunicazione all’interessato, di cui al precedente comma, se ricorre una delle seguenti condizioni:

- a) l’Università ha messo in atto 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 a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

6. Nel caso in cui l’Università non abbia comunicato all’interessato la violazione dei dati personali, il Garante per la protezione dei dati personali, 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 precedente comma 5 è soddisfatta.

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

8. Ciascun dipendente o collaboratore (a vario titolo) dell’Università è tenuto a conformarsi alle ulteriori regole e istruzioni che sono state adottate dall’Università con il provvedimento generale del settembre 2021 (c.d. “Procedura per la gestione delle violazioni di dati personali), dovendo, in ogni caso, garantire una costante cooperazione e a comunicare agli uffici preposti tutte le informazioni utili alla gestione della violazione dei dati personali.

TRASPARENZA E TUTELA DELL’INTERESSATO

Art. 22 – INFORMAZIONI ALL’INTERESSATO

1. L’Università, ogniqualvolta provvede alla raccolta di dati personali presso l’interessato, fornisce all’interessato le seguenti informazioni:

- l’identità e i dati di contatto del titolare del trattamento;
- i dati di contatto del D.P.O.;
- le finalità del trattamento cui sono destinati i dati personali e la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l’eventuale intenzione del titolare del trattamento di trasferire dati personali a un Paese terzo o a un’organizzazione internazionale e l’esistenza o l’assenza di una decisione di adeguatezza della Commissione o, in mancanza di una decisione di adeguatezza della Commissione, il riferimento alle garanzie appropriate o opportune (artt. 46, 47 e 49 del Regolamento (UE) n. 679 del 2016) e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

2. In aggiunta alle informazioni indicate al precedente comma, l’Università nel momento in cui i dati personali sono ottenuti, fornisce all’interessato le seguenti ulteriori informazioni:

- il periodo di conservazione dei dati personali oppure, se non è possibile indicare il periodo, i criteri utilizzati per determinarlo;
- i diritti riconosciuti dalla legge in capo all’interessato e le modalità di esercizio di tali diritti;
- se il trattamento è basato sul consenso dell’interessato, l’esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- se la fornitura dei (propri) dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l’interessato ha l’obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata fornitura di tali dati;
- il diritto di proporre reclamo al Garante per la protezione dei dati personali a tutela dei suoi diritti;
- 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.

3. Se la raccolta dai dati non avviene presso l’interessato, l’Università fornisce al medesimo, in aggiunta alle indicazioni di cui ai precedenti commi, le seguenti informazioni attinenti:

- alle categorie di dati trattati;
- alla fonte da cui i dati hanno origine e, se del caso, all’eventualità che i dati provengano da fonti accessibili al pubblico.

4. Nel caso di dati personali che sono stati raccolti presso l’interessato, l’Università fornisce all’interessato le informazioni nel momento in cui i dati personali sono ottenuti. Nel caso di dati personali che non sono stati raccolti presso l’interessato, l’Università fornisce le informazioni all’interessato:

- entro un termine ragionevole dall’ottenimento dei dati personali e, in ogni caso, entro un mese;
- se i dati sono finalizzati alla comunicazione con l’interessato, non oltre la prima comunicazione con lo stesso;
- se è prevista la comunicazione dei dati ad altro destinatario, non oltre la prima comunicazione al medesimo.

5. Se i dati personali sono stati raccolti presso l’interessato, l’Università non è tenuta a fornire le informazioni indicate nei precedenti commi 1° e 2° se, e nella misura in cui, queste informazioni siano già

in possesso dell’interessato. Se i dati personali non sono stati raccolti presso l’interessato, l’Università non è tenuta a fornire le informazioni indicate nei precedenti commi 1°, 2° e 3° se e nella misura in cui:

- queste informazioni sono già in possesso dell’interessato;
- la comunicazione all’interessato risulta impossibile;
- la comunicazione all’interessato implica uno sforzo sproporzionato, in particolare nel caso di trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o a fini statistici, ferma restando l’adozione di garanzie adeguate per i diritti e le libertà dell’interessato e di misure tecniche e organizzative, come la pseudonimizzazione, che assicurino il rispetto del principio di minimizzazione dei dati;
- la comunicazione all’interessato rischia di pregiudicare gravemente il conseguimento delle finalità del trattamento, ferma restando l’adozione di misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato, anche rendendo pubbliche le informazioni;
- l’ottenimento dei dati è espressamente previsto da norma comunitaria o nazionale che prevede misure appropriate per tutelare gli interessi legittimi dell’interessato;
- i dati personali devono rimanere riservati per un obbligo di segreto professionale o un obbligo di segretezza previsto per legge.

6. Le informazioni sono fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, anche con mezzi elettronici. Le informazioni all’interessato sono fornite per iscritto o con altri mezzi, anche elettronici. Se richiesto dall’interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi la sua identità.

7. Qualora l’Università intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati originariamente raccolti, prima di tale ulteriore trattamento fornisce all’interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

8. Al fine di garantire uniformità nella predisposizione delle informative sul trattamento dei dati personali, da fornire all’interessato conformemente a quanto indicato nei precedenti commi, la Commissione permanente d’Ateneo per l’applicazione del Regolamento (UE) n. 679 del 2016 ha elaborato un modello di informativa sul trattamento dei dati personali.

9. Anche al fine di garantire la trasparenza delle misure adottate a tutela dell’interessato, le principali informative sul trattamento dei dati personali sono state pubblicate sul sito istituzionale dell’Ateneo.

Art. 23 - DIRITTI DELL’INTERESSATO

1. L’Università garantisce all’interessato i diritti riconosciutigli dagli artt. 15 - 22 del Regolamento (UE) n. 679 del 2016. In particolare, l’interessato può:

- ottenere la conferma dell’esistenza o meno di dati personali che lo riguardano e l’accesso alle informazioni indicate dall’art. 15 del Regolamento (UE) n. 679 del 2016, fra cui le finalità del trattamento e le categorie di dati;
- ottenere una copia dei dati personali oggetto di trattamento, anche tramite formato elettronico di uso comune;
- ottenere senza ingiustificato ritardo la rettifica dei dati inesatti e l’integrazione dei dati incompleti;
- ricorrendone i presupposti di legge e nei limiti previsti, ottenere senza ingiustificato ritardo la cancellazione dei dati;
- ricorrendone i presupposti di legge e nei limiti previsti, ottenere la limitazione del trattamento;
- ricorrendone i presupposti di legge e nei limiti previsti, ottenere il trasferimento dei dati personali ad altro titolare del trattamento;
- opporsi al trattamento;
- proporre reclamo a un’Autorità di controllo;
- proporre ricorso all’Autorità Giudiziaria.

2. L’interessato può esercitare i diritti riconosciutigli dal Regolamento (UE) n. 679 del 2016, inoltrando una richiesta al titolare del trattamento, avvalendosi di una delle seguenti modalità:

- tramite comunicazione via p.e.c. all’indirizzo ateneo@pec.unich.it;
- tramite comunicazione via e-mail all’indirizzo: rettore@unich.it;

- tramite comunicazione all’indirizzo: Università G. d’Annunzio di Chieti-Pescara, Via dei Vestini 31, Chieti.

L’interessato può altresì esercitare i diritti riconosciutigli dal Regolamento (UE) n. 679 del 2016, inoltrando una richiesta al D.P.O., tramite comunicazione via e-mail all’indirizzo dpo@unich.it o via p.e.c. all’indirizzo dpo@pec.unich.it.

Alla richiesta deve essere, a tutela dell’interessato, allegata copia di un documento di identità in corso di validità.

3. L’istanza può essere presentata da un delegato dell’interessato, che esibisce o allega copia della procura o della delega sottoscritta, unitamente a copia fotostatica non autenticata di un documento di riconoscimento proprio e dell’interessato.

4. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell’interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione. È fatto salvo il caso in cui l’interessato abbia manifestato in modo non equivoco la volontà specifica, libera e informata di vietare l’esercizio dei diritti o di alcuni di essi.

5. La richiesta dell’interessato viene soddisfatta senza ingiustificato ritardo e comunque nel termine massimo di 1 mese dal ricevimento della richiesta, prorogabile di ulteriori 2 mesi se necessario, tenuto conto della complessità e del numero delle richieste. L’interessato è informato della proroga e dei motivi del ritardo entro 1 mese dal ricevimento della richiesta.

6. L’Università comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate in riscontro a richieste dell’interessato, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all’interessato tali destinatari qualora l’interessato lo richieda.

7. L’esercizio dei diritti è gratuito, salvi i casi di richieste manifestamente infondate, pretestuose o eccessive, anche per il loro carattere ripetitivo, per le quali potrà essere addebitato un contributo spese ragionevole, tenuto conto dei costi amministrativi sostenuti dall’Università oppure l’Università potrà rifiutare di dare riscontro alla richiesta. Incombe sull’Università l’onere di dimostrare il carattere manifestamente infondato, pretestuoso o eccessivo della richiesta.

TIPOLOGIE, OGGETTO DEI TRATTAMENTI E (LORO) FINALITÀ

Art. 24 - TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

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 di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale o all’orientamento sessuale della persona è ammesso solo in presenza di una delle condizioni di cui all’art. 9 del Regolamento (UE) n. 679 del 2016, di seguito elencate:

- l’interessato ha prestato il consenso esplicito al trattamento dei dati per una o più finalità specifiche;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti dell’Università o dell’interessato in materia di diritto del lavoro, sicurezza e protezione sociale;
- 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;
- il trattamento riguarda dati personali resi manifestamente pubblici dall’interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- 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;
- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, in conformità dell’art. 89, par. 1° del Regolamento (UE) n. 679 del 2016;

- 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.

2. Secondo quanto previsto dall’art. 2-sexies del Codice in materia di protezione dei dati personali, si considerano, fra le altre, di rilevante interesse pubblico i trattamenti eseguiti nelle seguenti materie:

- accesso a documenti amministrativi e accesso civico;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- obiezione di coscienza;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
- compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- programmazione, gestione, controllo e valutazione dell’assistenza sanitaria, ivi incluse l’instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l’amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
- tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
- istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materiale sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell’ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, tutela del patrimonio informativo dell’Ateneo, igiene e sicurezza di lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

3. I dati genetici, biometrici e relativi alla salute possono essere trattati solo in presenza di una delle condizioni indicate al precedente comma 1 e in conformità alle misure di garanzia disposte dal Garante per la protezione dei dati personali. I dati di cui al presente comma non possono in nessun caso essere diffusi.

Art. 25 - TRATTAMENTO DI DATI RELATIVI A CONDANNE PENALI E REATI

1. Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è ammesso solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati, riguardanti in particolare:

- l’adempimento di obblighi e l’esercizio di diritti da parte del titolare o dell’interessato nell’ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi;
- l’adempimento di obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione di controversie civili e commerciali;
- la verifica o accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
- l’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;
- l’accertamento, esercizio o difesa di un diritto in sede giudiziaria;
- l’esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
- l’adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità

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

- l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
- l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminosi e di finanziamento del terrorismo.

Art. 26 - TRATTAMENTO DI DATI PERSONALI NELL'AMBITO DEL RAPPORTO DI LAVORO

1. L'Università tratta i dati personali strumentali alla gestione del rapporto di lavoro, adottando misure appropriate a garantire la protezione dei diritti e delle libertà delle persone fisiche, delle prerogative sindacali e nel rispetto della legge, in particolare dello Statuto dei lavoratori, nonché dei contratti collettivi e delle regole deontologiche adottate dal Garante per la protezione dei dati personali
2. Il trattamento dei dati personali non richiede il consenso dell'interessato, in quanto è necessario all'esecuzione di un contratto di cui l'interessato è parte, all'esecuzione di misure precontrattuali adottate su richiesta dell'interessato, ad ottemperare a richieste dall'interessato, nonché per assolvere gli obblighi ed esercitare i diritti specifici dell'Università, quale titolare del trattamento, o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
3. L'Università garantisce al dipendente (o collaboratore a vario titolo) il diritto di accesso ai dati valutativi a questi riferiti.
4. Nei casi di ricezione di *curricula* spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile, successivo all'invio del *curriculum*.
5. Le disposizioni del presente articolo si applicano ai casi di collaborazione, consulenza, attività professionale comunque prestata a favore dell'Università.
6. Al trattamento di dati personali di cui al presente articolo si applicano le disposizioni di cui al Regolamento dell'utilizzo della rete di Ateneo, dei servizi e della posta elettronica.

Art. 27 - TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

1. Le strutture e le articolazioni dell'Università operanti in ambito sanitario o della prevenzione e sicurezza del lavoro, con esclusione di quelle di cui al successivo comma 5, trattano dati personali idonei a rivelare lo stato di salute se necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, gestione dei sistemi e servizi sanitari o sociali ovvero per motivi di interesse pubblico nel settore della sanità pubblica, sulla base di una norma di legge o di regolamento o del diritto dell'Unione Europea. Il trattamento è effettuato da un professionista soggetto al segreto professionale, o sotto la sua responsabilità, in conformità alle misure di garanzia disposte dal Garante per la protezione dei dati personali e alle specifiche disposizioni di settore.
2. Le strutture e le articolazioni di cui al precedente comma 1 possono adottare modalità semplificate per fornire all'interessato l'informativa sul trattamento dei dati personali.
3. Le informazioni riguardanti il trattamento dei dati personali possono essere rese, senza ritardo, successivamente alla prestazione in caso di:
 - impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le informazioni a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, familiare, convivente, unito civilmente, fiduciario o responsabile della struttura presso cui dimora l'interessato;
 - rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato;
 - prestazione medica che può essere pregiudicata dal preventivo rilascio delle informazioni, in termini di tempestività o efficacia.

Dopo il raggiungimento della maggiore età, le informazioni sul trattamento dei dati personali sono fornite all’interessato, se non già rilasciate in precedenza.

4. Fermo restando quanto previsto dalle norme di legge e di regolamento in materia di trattamento di categorie particolari di dati personali, in relazione ai trattamenti di dati personali di cui al presente articolo sono adottate le seguenti misure a garanzia del rispetto dei diritti dell’interessato:

- a) distanze di cortesia e soluzioni che prevengano l’indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
- b) specifiche cautele per evitare l’erogazione delle prestazioni in situazioni di promiscuità;
- c) accorgimenti volti ad assicurare che la notizia, inerente allo stato di salute, sia data al solo interessato o ai soli terzi a ciò legittimati;
- e) rispetto della dignità dell’interessato in occasione della prestazione medica e in ogni operazione di trattamento;
- f) sottoposizione a regole di condotta analoghe al segreto professionale di tutti coloro che effettuano trattamenti di dati personali in ambito sanitario.

5. Nell’ambito di applicazione del precedente comma 1 non rientrano le strutture universitarie afferenti alla Scuola di Medicina e Scienze della Salute convenzionate con il Servizio Sanitario Nazionale, che trattino i dati personali, anche di natura sanitaria, per conto dell’azienda ospedaliera di riferimento, titolare del trattamento, fermo restando che rispetto a dette strutture trovano applicazione le leggi e i regolamenti che disciplinano i trattamenti di dati personali da parte degli organismi sanitari pubblici, nonché le specifiche disposizioni impartite dal titolare del trattamento.

ART. 28 - TRATTAMENTO DI DATI PERSONALI PER FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE O DI RICERCA STORICA

- 1. I documenti contenenti dati personali trattati a fini di archiviazione nel pubblico interesse o di ricerca storica sono utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il raggiungimento di tali scopi e sempre che, nel rispetto del principio di minimizzazione del trattamento, non sia possibile utilizzare dati anonimi o procedere alla pseudonimizzazione.
- 2. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non sono utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all’interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell’art. 5 del Regolamento (UE) n. 679 del 2016.
- 3. Il trattamento dei dati personali ai fini del presente articolo è effettuato altresì nel rispetto delle regole deontologiche in materia approvate dal Garante per la protezione dei dati personali.
- 4. La consultazione dei documenti di interesse storico conservati negli archivi dell’Università è disciplinata dal d.lgs. n. 42 del 2004 e dalle succitate relative regole deontologiche.

ART. 29 - TRATTAMENTO DI DATI PERSONALI A FINI STATISTICI O DI RICERCA SCIENTIFICA

- 1. Il trattamento di dati personali a 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 delle garanzie previste dalle regole deontologiche approvate in materia dal Garante per la protezione dei dati personali ed in particolare nel rispetto dei seguenti principi:
 - i dati personali non possono essere trattati per prendere decisioni o provvedimenti relativamente all’interessato, né per scopi diversi da quelli per i quali sono stati originariamente raccolti;
 - all’interessato deve essere fornita una chiara e completa informativa sul trattamento dei dati personali, a meno che questo adempimento 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;
 - le particolari categorie di dati personali e i dati relativi a condanne penali e reati devono di regola essere trattati in forma anonima. Si può procedere con il trattamento di particolari categorie di dati personali solo con il consenso, manifestato per iscritto, dell’interessato. Quando la raccolta delle categorie particolari di

dati personali è effettuata con modalità che rendono particolarmente gravoso l’acquisizione per iscritto, il consenso dell’interessato, purché esplicito, può essere documentato per iscritto;

- i dati personali devono essere conservati non oltre il periodo necessario alle finalità della raccolta e con modalità idonee da evitarne la perdita, la distruzione, l’accesso non autorizzato e ogni altro uso non conforme alla normativa vigente.

ART. 30 - TRATTAMENTO DI DATI PERSONALI A FINI DI RICERCA MEDICA, BIOMEDICA ED EPIDEMIOLOGICA

1. Il consenso dell’interessato per il 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’art. 12-*bis* del d.lgs. n. 502 del 1992, e sia condotta e resa pubblica una valutazione di impatto sulla protezione dei dati personali, ai sensi degli artt. 35 e 36 del Regolamento (UE) n. 679 del 2016 e dell’art. 18 del presente regolamento.

2. Il consenso dell’interessato al trattamento dei dati relativi alla salute per le finalità indicate al precedente comma non è altresì necessario quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato oppure vi sia un rischio reale di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In questi casi, l’Ateneo in qualità di titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato e documenta i ragionevoli sforzi profusi per tentare di contattare l’interessato. Il progetto di ricerca è oggetto di motivato parere favorevole del Comitato etico competente a livello territoriale, salvo che la legge non riservi la competenza ad altro comitato etico, e deve essere, comunque, sottoposto alla valutazione di impatto sulla protezione dei dati.

3. In caso di esercizio del diritto di rettifica e di 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.

4. Ai fini del trattamento ulteriore da parte di soggetti terzi dei dati personali di cui al presente articolo si applica quanto disposto dall’art. 110-*bis* del Codice in materia di protezione dei dati personali.

Art. 31 - TRATTAMENTO DI DATI PERSONALI NELLE SEDUTE DEGLI ORGANI COLLEGIALI

1. Nelle sedute degli organi collegiali dell’Università, il trattamento dei dati personali avviene in conformità alla normativa vigente e al presente regolamento e, conseguentemente, nella misura in cui il trattamento di dati personali sia necessario all’espletamento delle attività di competenza degli organi.

2. La pubblicazione dei dati personali contenuti nelle deliberazioni degli organi collegiali è ammessa solo ove questa operazione sia prevista dalla legge o sia strettamente necessaria al perseguimento delle finalità istituzionali dell’Università.

3. La pubblicazione dei dati personali contenuti nelle deliberazioni degli organi collegiali, ove prevista, avverrà nel rispetto dei principi di necessità e di pertinenza sanciti dall’art. 5 del Regolamento (UE) n. 679 del 2016

Art. 32 - COMUNICAZIONE E DIFFUSIONE DI DATI PERSONALI

1. L’Università può comunicare dati personali, diversi da quelli particolari di cui all’art. 9 del Regolamento (UE) n. 679 del 2016 e relativi a condanne penali e reati, nei seguenti casi:

- comunicazione fra titolari che effettuano trattamenti per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri, se previsto da norme di legge, di regolamento o dal diritto dell’Unione Europea. In mancanza di tali norme, la comunicazione è ammessa se necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata decorso il termine di quarantacinque giorni dalla comunicazione al Garante per la protezione dei dati

personali, senza che lo stesso abbia adottato una diversa determinazione delle misure a garanzia degli interessati;

- comunicazione necessaria per finalità di difesa o sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, nel rispetto delle norme che regolano la materia;
- comunicazione necessaria per il soddisfacimento di richieste di accesso ai documenti amministrativi ai sensi della legge n. 241 del 1990 o di esercizio, anche ad opera di soggetti terzi, dei diritti dell’interessato;
- comunicazione di dati relativi agli esiti formativi intermedi e finali di studenti, diplomati, laureati, specializzati, borsisti, dottorandi, assegnisti e di altri profili formativi, nonché di soggetti che hanno superato l’esame di Stato, e di altri dati personali, comunque pertinenti in relazione alla finalità di agevolare l’orientamento, la formazione e l’inserimento professionale, anche all’estero, degli studenti e dei laureati dell’Ateneo;
- comunicazione a soggetti finanziatori di borse di dottorato e di assegni alla ricerca di dati personali relativi ai dottorandi e agli assegnisti che abbiano usufruito dei finanziamenti;
- comunicazione ad altre pubbliche amministrazioni e diffusione, anche tramite pubblicazione sul sito istituzionale dell’Università, dei nominativi del personale e dei collaboratori, del ruolo ricoperto, dei recapiti telefonici e degli indirizzi telematici istituzionali, al fine di favorire la comunicazione istituzionale;
- comunicazione ad enti pubblici e privati di dati necessari alla gestione del rapporto di lavoro;
- comunicazione alle aziende ospedaliere in convenzione dei dati personali inerenti al personale che eserciti la propria attività nell’ambito della convenzione con tali enti;
- comunicazione a soggetti pubblici e privati che organizzano e gestiscono corsi di formazione e di aggiornamento professionale dei dati del personale che partecipa, a qualunque titolo, a tali corsi.

2. Le richieste rivolte all’Università per ottenere la comunicazione di dati personali devono essere indirizzate per iscritto al responsabile della struttura e devono contenere:

- il nome, la denominazione o la ragione sociale del richiedente;
- i dati cui la domanda si riferisce, le finalità e le modalità di utilizzo dei dati richiesti;
- la dichiarazione che il richiedente si impegna a utilizzare i dati ricevuti esclusivamente per le finalità per cui sono stati richiesti.

Il responsabile della struttura, anche tramite il supporto dell’Ufficio Privacy di Ateneo e il D.P.O., valuta la legittimità della richiesta e, in caso di esito positivo, autorizza la comunicazione dei dati nella misura e nelle modalità strettamente necessarie a soddisfare la richiesta medesima.

3. In attuazione del principio di trasparenza, è consentita la pubblicazione dei dati inerenti alle valutazioni di esame anche sul sito istituzionale dell’Ateneo, in una sezione accessibile utilizzando le personali credenziali di accesso fornite dall’Ateneo. La pubblicazione dei dati è consentita unicamente mediante l’indicazione del numero di matricola dello studente e del voto conseguito. I dati sono resi disponibili per un periodo di tempo non superiore all’anno accademico di riferimento.

4. L’Università è tenuta a pubblicare gli esiti delle procedure di reclutamento del personale, delle procedure di selezione per l’ammissione a corsi a numero programmato o per il conferimento di assegni di ricerca, borse di dottorato o di studio, incarichi di collaborazione e/o insegnamento, nonché le relative graduatorie, anche sul sito istituzionale dell’Ateneo. La pubblicazione dei dati è effettuata in ogni caso nel rispetto dei principi generali sanciti dall’art. 5 del Regolamento (UE) n. 679 del 2016, mediante l’indicazione dei soli dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati. I dati sono resi disponibili per un periodo di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono stati pubblicati.

ART. 33 – TRATTAMENTO DI IMMAGINI

1. Non è necessario il consenso dell’interessato quando il trattamento della (sua) immagine è giustificato da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico.

2. Il trattamento delle immagini, ancorché raccolte per scopi scientifici, didattici o culturali o comunque effettuato nell’ambito di eventi di interesse pubblico o svoltisi in pubblico, deve essere preceduto dall’informativa sul trattamento dei dati personali.
3. Laddove non sia possibile fornire l’informativa prima dell’evento, la stessa è messa a disposizione dei partecipanti, dando evidenza del trattamento tramite affissione di un avviso nel luogo dell’evento stesso.
4. Il trattamento di cui al presente articolo avviene, in ogni caso, nel rispetto della dignità delle persone, evitando la riproduzione di immagini che siano lesive dell’onore e della reputazione dell’interessato.
5. Non è possibile riprodurre le immagini di un minore se non con il consenso, manifestato per iscritto, dai soggetti esercenti la responsabilità genitoriale.

Art. 34 - VIDEOSORVEGLIANZA

1. L’Università procede al trattamento di dati personali attraverso sistemi di videosorveglianza strumentali all’esercizio delle proprie finalità istituzionali. I dati personali raccolti tramite i sistemi di videosorveglianza, compresi evidentemente le immagini, sono trattati nel rispetto dei diritti e delle libertà fondamentali dell’interessato e in osservanza del principio di minimizzazione sancito dall’art. 5 del Regolamento (UE) n. 679 del 2016. Nel rispetto del principio di pertinenza e di non eccedenza nel trattamento dei dati personali, i dati personali, raccolti tramite sistemi di videosorveglianza, sono trattati esclusivamente per le finalità di seguito indicate:
 - a) garantire la sicurezza e l’incolumità del personale amministrativo e docente, degli studenti e dei frequentatori a vario titolo degli spazi dell’Università;
 - b) tutelare il patrimonio dell’Università.
2. Nelle strutture dove sono in funzione sistemi di videosorveglianza, deve essere affissa, in modo visibile dall’interessato e prima di entrare nel raggio di operatività delle videocamere, apposita informativa, redatta sulla base del modello di informativa semplificata proposta dal Garante, che informi l’utenza e il pubblico della presenza degli impianti, del nominativo del titolare del trattamento e delle finalità perseguite.
3. L’Università garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza adottando le misure di sicurezza di seguito indicate:
 - a) ai dati registrati possono accedere esclusivamente soggetti appositamente designati autorizzati al trattamento e a cui sono state fornite dettagliate istruzioni operative ed organizzative;
 - b) i dati registrati non possono essere utilizzati per finalità diverse da quelle perseguite dall’Università;
 - c) i dati registrati sono conservati per il solo tempo necessario alle finalità cui la registrazione è strumentale e, in ogni caso, per un tempo non superiore alle 48 (quarantotto) ore successive alla rilevazione, fatta salva l’ipotesi in cui vi sia una specifica richiesta dell’autorità giudiziaria o di pubblica sicurezza, l’ipotesi di chiusura programmata delle strutture dell’Università o l’ipotesi di sopravvenute esigenze il cui soddisfacimento potrebbe richiedere tempi più lunghi di conservazione.
4. Per quanto non espressamente previsto nel presente articolo, si rinvia ai provvedimenti del Garante per la protezione dei dati personali adottati in materia e disponibili sul sito istituzionale dell’Autorità, nonché alle Linee Guida n. 3 del 2019 sul trattamento dei dati personali attraverso dispositivi video, adottate dal Comitato europeo per la protezione dei dati personali.

NORME FINALI

Art. 35 – SANZIONI

Fermo restando quanto previsto dagli artt. 58, 82, 83 e 84 del Regolamento (UE) n. 679 del 2016 e dagli artt. 166 – 168 del Codice in materia di protezione dei dati personali, le sanzioni disciplinari a carico del personale in caso di violazione delle leggi, del presente regolamento, delle linee guida, delle *policy* e delle

procedure in tema di protezione dei dati personali saranno definite dall’Ateneo, anche sulla base di quanto disposto dal Codice etico dell’Università G. d’Annunzio di Chieti-Pescara.

Art. 36 – ENTRATA IN VIGORE E RINVII

1. Il presente Regolamento ed eventuali sue successive modifiche, deliberati dal Consiglio di amministrazione, previo parere favorevole del Senato accademico, sono emanati con decreto del Rettore ed entrano in vigore il giorno successivo a quello della sua pubblicazione sul sito istituzionale dell’Università.
2. Per quanto non espressamente previsto dal presente Regolamento, si rinvia alla normativa europea e nazionale in materia, nonché ai provvedimenti e alle regole deontologiche adottati dal Garante per la protezione dei dati personali.