UNIVERSITÀ DEGLI STUDI DI BRESCIA

DECRETO

Oggetto: Emanazione “Regolamento in materia di Protezione dei dati personali”

IL RETTORE

VISTO:

- il D.Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
- il D.Lgs. n. 33 del 14 marzo 2013, "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- il Regolamento UE 2016/679 - GDPR (*General Data Protection Regulation*), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali adottato il 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale dell'Unione europea il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018;
- lo Statuto dell’Università degli Studi di Brescia, emanato con D.R. del 6 febbraio 2024, n. 107 e pubblicato in Gazzetta Ufficiale del 16 febbraio 2024 n. 39;
- il testo del Regolamento in materia di protezione dei dati personali (All.1), condiviso con il Responsabile esterno della Protezione Dati, Liguria Digitale spa, nominato con D.R. n. 1241/2023 del 21 dicembre 2023;

RICHIAMATA la delibera del Senato Accademico n. 166/2024 del 24 giugno 2024, prot.155039, con la quale si esprime parere favorevole alla modifica del Regolamento in materia di protezione dei dati personali (privacy), emanato con D.R. n. 473 del 31 ottobre 2013;

RICHIAMATA la delibera del Consiglio di Amministrazione n. 158/2024 del 25 giugno 2024, prot.155198, con la quale si approva il nuovo Regolamento in materia di protezione dei dati personali (privacy);

DECRETA

per le motivazioni indicate nelle premesse del presente atto e che qui si intendono integralmente riportate, l’emanazione del “Regolamento in materia di Protezione dei dati personali”, che entrerà in vigore il primo giorno feriale successivo alla pubblicazione all’albo on-line di Ateneo, allegato al presente Decreto, di cui fa parte integrante e sostanziale.

Brescia, data protocollo

IL RETTORE
(Prof. Francesco Castelli)

F.to digitalmente ex art. 24 D.Lgs 82/05

Firmato digitalmente da Francesco Castelli
Data: 01.07.2024 08:24:51 CEST
Organizzazione: UNIVERSITA' DEGLI STUDI DI BRESCIA/01773710171

U.A.S. Protezione dei Dati - RPD
Il Responsabile del Procedimento: Antonio Zuccaro

UNIVERSITÀ DEGLI STUDI DI BRESCIA

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

INDICE

CAPO I - Oggetto e principi

Art. 1 - Oggetto

1. L'Università degli Studi di Brescia – di seguito Università o Ateneo – tratta i dati personali in conformità a quanto previsto dal Regolamento UE n. 2016/679 (Regolamento Generale sulla protezione dei dati, di seguito "GDPR"), e del Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice *privacy*"), come modificato dal Decreto legislativo 10 agosto 2018, n. 101.

2. I dati sono trattati nel rispetto dei diritti e delle libertà fondamentali dell'interessato.

3. L'Università considera il trattamento lecito, corretto e trasparente dei dati personali, come previsto dall'art. 5 GDPR, un'azione prioritaria al fine di instaurare e mantenere un rapporto di fiducia con gli studenti, il personale e i terzi interessati.

4. I trattamenti effettuati dall'Università per il raggiungimento dei propri fini istituzionali non necessitano del consenso dell'interessato, fatti salvi i casi previsti dalla legge, e rinvengono la propria base giuridica nell'art. 6 del GDPR.

5. Nel caso di trasferimento di dati personali verso un paese terzo (anche extra UE) o un'organizzazione internazionale, l'Università è responsabile del rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione dei dati delle persone fisiche garantito dal GDPR, al Capo V, art. 44 e ss.

Art. 2 – Definizioni

1. Ai fini del presente regolamento, si intende per:

a) *"dato personale"*: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("*c.d. interessato*");
b) *"trattamento"*: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, l'elaborazione, 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, l'allineamento o la combinazione, la cancellazione o la distruzione;
c) *"consenso dell'interessato"*: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
d) *"comunicazione"*: il dare conoscenza dei dati personali a uno o più soggetti determinati in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
e) *"diffusione"*: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
f) *"violazione dei dati personali"* – c.d. *"data breach"*: la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o, comunque, trattati dall'Università;

g) *"profilazione"*: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
h) *"pseudonimizzazione"*: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
i) *"autorizzati"*: le persone fisiche che hanno con l'Ateneo rapporti di lavoro, servizio, collaborazione, studio o ricerca e che sono formalmente autorizzate e istruite dal titolare al trattamento dei dati personali.

2. Per le ulteriori definizioni si rinvia all'art. 4 del GDPR.

Art. 3 - Principi

1. L'Università è una pubblica amministrazione, persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche.

2. Il trattamento dei dati personali è effettuato in applicazione dei principi previsti dall'art. 5 del GDPR. In particolare, i dati personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**liceità, correttezza e trasparenza)**;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità (**limitazione della finalità**);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**minimizzazione dei dati**);
- 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)**;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, a condizione dell'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR e dal presente regolamento (**limitazione della conservazione**);
- 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**);
- trattati sempre in quanto necessari al perseguimento dei fini per i quali il trattamento viene lecitamente effettuato (**necessità)**.

3. La protezione dei dati personali è garantita fin dalla fase di progettazione del trattamento degli stessi e dell'adozione delle relative misure di sicurezza (*privacy by design*). Sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (*privacy by default*).

Art. 4 - Formazione del personale

1. L'Università sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo promuove l'attività informativa e formativa del personale universitario e la diffusione delle informative.

2. L'Università, sentito l'RPD, inserisce nel proprio piano formativo corsi in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione (*data breach*), al fine di garantire una gestione delle attività di trattamento responsabile, informata e aggiornata.

3. La formazione è obbligatoria e ogni sessione può prevedere una prova finale di apprendimento.

CAPO II - Ruoli e compiti

Art. 5 - Titolare del trattamento dei dati

1. Il titolare del trattamento dei dati è l'Università degli Studi di Brescia rappresentata dal Rettore *pro tempore*. Il titolare:

a) definisce, mette in atto, riesamina e, ove necessario, aggiorna le misure tecniche e organizzative adeguate ed efficaci per garantire ed essere in grado di dimostrare che ogni trattamento dei dati personali è effettuato conformemente ai principi e alle disposizioni del GDPR, del Codice *privacy* e della normativa applicabile in materia;
b) adotta il provvedimento di nomina dei responsabili e dei referenti di cui agli artt. 8 e 9 del presente regolamento, con l'indicazione analitica dei compiti affidati a ciascuno di essi;
c) accerta periodicamente la puntuale osservanza delle disposizioni scritte impartite ai responsabili del trattamento e ai referenti del trattamento;
d) ornisce le informative sul trattamento dei dati all'interessato;
e) è responsabile del registro delle attività di trattamento, di cui all'art. 30 GDPR (cfr. art. 24 del presente regolamento);
f) dà seguito alle richieste per l'esercizio dei diritti dell'interessato, di cui agli artt. 15-22 GDPR (cfr. art. 25 del presente regolamento);
g) effettua la valutazione di impatto sulla protezione dei dati ogniqualvolta un trattamento preveda l'uso di nuove tecnologie che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 35 GDPR;
h) ai sensi degli artt. 33 e 34 GDPR, notifica al Garante per la protezione dei dati personali (di seguito Garante) le violazioni di dati personali;
i) valuta la necessità di comunicare all'interessato le violazioni di dati personali;
j) promuove la formazione generale e specifica del personale.

2. Con riguardo al Responsabile della protezione dei dati personali di cui all'art. 7, il titolare del trattamento:

a) provvede alla sua nomina (cfr. GDPR artt. 37 e 38);
b) istituisce una struttura di supporto e mette a disposizione ogni risorsa al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate;
c) non lo rimuove o penalizza in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
d) garantisce che eserciti le proprie funzioni in autonomia e indipendenza, in particolare non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse.

Art. 6 - Contitolare del trattamento

1. Ove l'Università determini le finalità e i mezzi di un trattamento dei dati congiuntamente ad un altro titolare del trattamento – pubblico o privato –, tale soggetto diviene contitolare del trattamento, ai sensi dell'art. 26 GDPR.

2. L'Università e il contitolare determinano in modo trasparente, mediante un accordo specifico (c.d. accordo di contitolarità), le rispettive responsabilità in relazione all'osservanza degli obblighi derivanti dal GDPR e dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, alla gestione di eventuali *data breach* e alle rispettive funzioni di comunicazione ai soggetti interessati dal trattamento, in merito alla sottoposizione dell'informativa al trattamento dei dati personali, ai sensi degli artt. 13 e 14 GDPR.

3. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti del contitolare con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

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

Art 7 - Responsabile della protezione dei dati personali

1. Il Responsabile della protezione dei dati personali (RPD) o *Data Protection Officer* (DPO), di seguito "RPD":

a) è figura specializzata nel supporto al titolare del trattamento e svolge la funzione di punto di contatto con il Garante per la protezione dei dati personali e di tutela per i soggetti interessati;
b) è individuato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui al comma 4;
c) può essere un soggetto interno o esterno.

2. L'RPD è nominato con decreto del Rettore.

3. L'incarico ha durata triennale ed è rinnovabile.

4. L'RPD svolge i seguenti compiti e funzioni:

a) informa e fornisce consulenza al titolare del trattamento, ai referenti, ai responsabili nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento, dal GDPR, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) vigila sull'osservanza del presente regolamento, del GDPR, di altre disposizioni nazionali o dell'Unione europea relative alla protezione dei dati nonché delle politiche del titolare in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo, anche per tramite del referente di cui all'art. 9;
c) fornisce parere in merito alla valutazione d'impatto sulla protezione dei dati;
d) coopera con il Garante *privacy*;
e) funge da punto di contatto con il Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
f) relaziona sull'attività svolta e sullo stato di attuazione in Ateneo della normativa sulla protezione dei dati personali, trasmettendola al Rettore e al Direttore Generale;
g) in caso di *data breach* svolge i compiti previsti dalla relativa procedura.

5. Il nominativo e i dati di contatto dell'RPD sono pubblicati sul sito internet istituzionale dell'Università e comunicati al Garante.

Art. 8 - Responsabile del trattamento dei dati personali

1. Il fornitore esterno, persona fisica o giuridica, che tratta dati personali per conto dell'Università, assume il ruolo di responsabile del trattamento, ai sensi dell'art. 28 GDPR.

2. La nomina del responsabile del trattamento dei dati è effettuata dal titolare del trattamento con provvedimento scritto che individui all'interno di un atto di nomina la natura, le finalità e la durata del trattamento, il tipo di dati personali trattati e le categorie di interessati e definisca gli obblighi del responsabile del trattamento, nel rispetto delle previsioni di cui all'art. 28, par. 3, del GDPR.

3. Il responsabile del trattamento dei dati non può nominare un sub-responsabile, senza previa autorizzazione scritta del titolare. Nel caso in cui nomini un sub-responsabile del trattamento dei dati per l'esecuzione di specifiche attività di trattamento per conto del titolare, nell'atto di nomina devono essere previsti, a carico di detto sub-responsabile, gli stessi obblighi in materia di protezione dei dati contenuti nell'atto di nomina adottato dal titolare. Qualora il sub- responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare l'intera responsabilità di tali obblighi.

4. Il responsabile del trattamento:

a) adotta, aggiorna e mette a disposizione dell'Università un registro di tutte le attività svolte per conto della medesima;
b) assiste e collabora pienamente ai fini dell'adempimento delle attività poste in essere in caso di *data breach*;
c) ove necessario, assiste a livello tecnico e organizzativo nello svolgimento della valutazione di impatto;

d) adempie a tutte le prescrizioni in tema di trattamento dei dati personali impartite dall'Università.

5. Qualora l'Ateneo sia nominato responsabile del trattamento, il titolare o suo referente sottoscrive il relativo atto di nomina, provvedendo al rispetto delle istruzioni ricevute dallo stesso e alle previsioni del presente regolamento.

Art. 9 - Referenti del trattamento dei dati personali

1. I referenti del trattamento dei dati personali (o anche designati) sono nominati con Decreto Rettorale.

2. I referenti sono formati dal titolare del trattamento riguardo al proprio ruolo, collaborano funzionalmente con l'RPD e in particolare:

a) conoscono e rispettano la normativa in materia di protezione dei dati personali;
b) osservano il patto di riservatezza e le istruzioni impartite dal titolare del trattamento;
c) vigilano sul rispetto della normativa e delle istruzioni impartite da parte dei dipendenti e collaboratori afferenti alla struttura di cui sono responsabili;
d) adottano le opportune misure di sicurezza per garantire la protezione dei dati personali trattati nell'ambito della struttura di cui sono responsabili;
e) provvedono, se incaricati, alla tenuta e all'aggiornamento del registro dei trattamenti di cui all'art. 24 del presente regolamento. Laddove non autorizzati ad agire sul registro dei trattamenti, comunicano all'RPD e al titolare del trattamento gli elementi essenziali del trattamento da inserire, aggiornare o cancellare;
f) tengono e aggiornano gli archivi di dati personali, cartacei e informatizzati, e dei server attivi gestiti in maniera autonoma dalla struttura di cui sono referenti;
g) aggiornano la modulistica di propria competenza;
h) nel caso di strutture didattiche e di ricerca, vigilano sul rispetto degli adempimenti previsti dall'Ateneo in materia di mappatura dei progetti di ricerca;
i) qualora ricevano segnalazioni di violazione di dati personali ne danno tempestiva comunicazione all'RPD e al titolare del trattamento con le modalità previste dalla procedura di *data breach*;
j) formulano proposte al titolare del trattamento circa i bisogni formativi del personale della propria struttura;
k) partecipano alle sessioni informative, formative e di sensibilizzazione in materia di protezione dei dati personali;
l) segnalano al titolare del trattamento e all'RPD ogni variazione organizzativa che può avere un impatto sulle modalità di trattamento dei dati;
m) per i trattamenti che hanno come base giuridica il consenso, predispongono le misure organizzative atte a garantire la conservazione della copia del consenso acquisito, sulla base del principio di *accountability* e ai sensi dell'art. 7, par. 1, GDPR;
n) nominano personale autorizzato al trattamento dei dati coloro che hanno rapporti di servizio, collaborazione, studio e ricerca con la struttura di riferimento, qualora le sottese attività siano connesse al trattamento di dati personali. A tal fine si avvalgono di uno schema tipo di autorizzazione, trasmettendo agli autorizzati le correlate istruzioni, anche avvalendosi di procedure informatiche.

3. In caso di modifiche che identifichino nuove strutture o di variazioni delle posizioni organizzative

nell'ambito dell'atto di organizzazione amministrativa e tecnica, si procede all'aggiornamento delle nomine con Decreto Rettorale.

Art. 10 - Autorizzato al trattamento

1. I soggetti autorizzati al trattamento dei dati personali ("o autorizzati") operano sotto la diretta autorità del referente ed effettuano, con riferimento alle attività di propria competenza, i trattamenti dei dati personali nel rispetto delle misure di sicurezza previste e delle istruzioni ricevute.

2. Gli autorizzati, in particolare:

a) prendono visione dell'atto di autorizzazione al trattamento dei dati personali, del patto di riservatezza, unitamente alle istruzioni impartite dal titolare del trattamento, al momento dell'instaurazione del rapporto di lavoro con l'Ateneo;
b) partecipano alle sessioni informative, formative e di sensibilizzazione in materia di protezione dei dati personali;
c) mantengono il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui vengono a conoscenza nello svolgimento delle proprie mansioni;
d) trattano i dati personali solo per il tempo necessario e per le finalità per le quali sono stati autorizzati;
e) non comunicano a terzi e non diffondono notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui siano venuti a conoscenza nella propria qualità di autorizzati;
f) segnalano con tempestività all'RPD eventuali anomalie, incidenti, furti, perdite accidentali di dati, informando il proprio referente.

3. Tutti coloro che trattano dati personali nell'ambito del rapporto con l'Ateneo sono comunque ritenuti autorizzati al trattamento dei dati e sono obbligati a osservare quanto previsto dal presente articolo anche in assenza di formale designazione.

CAPO III - Trattamento dei dati

Art. 11 - Circolazione dei dati all'interno dell'Università

1. L'accesso ai dati personali è ispirato al principio della libera circolazione delle informazioni all'interno dell'Università per il raggiungimento dei fini istituzionali.

2. L'Università organizza le informazioni e i dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione.

3. L'accesso ai dati personali da parte degli autorizzati è soddisfatto in via diretta e senza ulteriori formalità nella misura necessaria al perseguimento dell'interesse istituzionale, ferma restando la responsabilità personale derivante dall'utilizzo improprio dei dati e dalla violazione delle istruzioni ricevute.

Art. 12 - Trattamento di categorie particolari di dati personali

1. Il trattamento di dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica, di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona è consentito solo se ricorrono le condizioni di cui all'art. 9, commi 2 e 3 del GDPR.

2. Quando il trattamento dei dati di cui al comma 1 del presente articolo è necessario per motivi di interesse pubblico rilevante, ai sensi dell'art. 9, co. 2, lett. g), del GDPR, esso è consentito soltanto se previsto nell'ambito del diritto dell'Unione europea o, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. La rilevanza dell'interesse pubblico è valutata, tra l'altro, alla luce dell'art. 2-*sexies*, comma 2, lett. bb), del Codice *privacy*.

3. Fermo quanto previsto ai precedenti commi 1 e 2, il trattamento dei dati genetici, biometrici e relativi alla salute deve avvenire in conformità a quanto previsto dall'art. 2-septies, co. 8, d.lgs. 196/2003 nonché alle misure di garanzia disposte dal Garante con proprio provvedimento. I dati di cui al presente comma non possono essere diffusi.

Art. 13 -Trattamento dei dati relativi a studenti

1. Ove ricorrano i presupposti normativi, per agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, l'Università può comunicare o diffondere, una volta acquisito il consenso dagli interessati e per via telematica, dati relativi agli esiti formativi, intermedi e finali degli studenti in relazione alle predette finalità e ai compiti ad esse connesse, a esclusione delle categorie di dati di cui agli artt. 9 e 10 del GDPR.

2. L'Università può comunicare, a finanziatori di borse di dottorato e assegni, anche stranieri, dati personali relativi a dottorandi e assegnisti che abbiano usufruito dei finanziamenti.

Art. 14 - Diffusione delle valutazioni d'esame

1. Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, è consentita la pubblicazione dei dati inerenti alle valutazioni d'esame anche sul sito *web* istituzionale di Ateneo.

2. La pubblicazione dei dati è effettuata nel rispetto del principio della minimizzazione ai sensi dell'art. 5, par. 1, lett. c) GDPR, mediante la diffusione di quei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati, ove possibile mediante l'indicazione del numero di matricola o di un codice identificativo temporaneo al posto del nome e cognome.

3. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a quello necessario al raggiungimento delle finalità per le quali i dati personali stessi sono resi pubblici.

4. Gli esami, le altre verifiche di profitto e le prove finali per il conferimento del titolo svolti in modalità a distanza non sono oggetto di videoregistrazione.

Art. 15 – Didattica a distanza

1. Le attività didattiche svolte a distanza possono essere registrate e conservate sino alla fine dell'anno accademico cui si riferiscono. Un ulteriore periodo di conservazione è ammesso previo consenso degli interessati.

2. Qualora la registrazione avvenga in presenza di pubblico, il docente dichiara l'intenzione di registrare l'attività prima dell'inizio della stessa dando le indicazioni operative agli interessati che abbiano espresso un diniego.

3. Le registrazioni sono trattate secondo le indicazioni fornite dall'Ateneo con particolare riferimento alla loro diffusione.

Art. 16 - Trattamento ai fini di ricerca

1. Il trattamento dei dati personali nell'ambito delle attività di ricerca è svolto nel rispetto della normativa vigente e dei provvedimenti del Garante della *privacy*.

2. Il responsabile scientifico è tenuto a compilare la "Scheda Progetto relativa alla Protezione dei Dati" già nella fase di predisposizione del progetto di ricerca stessa.

3. Non è necessario il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico e biomedico, 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 rientri in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'art. 12-*bis* del D.Lgs. 30 dicembre 1992, n. 502 e sia condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del GDPR.

4. Il consenso non è altresì necessario quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure vi sia un rischio reale di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il responsabile scientifico della ricerca adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Il progetto di ricerca è sottoposto a preventiva consultazione del comitato etico universitario, se esistente, salvo che la legge non riservi la competenza ad altro Comitato etico.

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

6. Ai fini del trattamento ulteriore da parte di terzi dei dati personali di cui al presente articolo si applica quanto disposto dall'art. 110-*bis* del Codice *privacy*.

Art. 17 - Trattamento ai fini di archiviazione nel pubblico interesse o di ricerca storica

1. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.

2. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto del principio della minimizzazione dei dati e delle regole deontologiche in materia approvate dal Garante e può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

3. 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.

4. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità secondo i principi stabiliti dall'art. 5 del GDPR.

5. La consultazione dei documenti di interesse storico conservati negli archivi dell'Università è disciplinata dal D.Lgs. 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio", dalle relative regole deontologiche e dai regolamenti di Ateneo in materia.

Art. 18 - Trattamento dei dati contenuti nei *curricula*

1. I dati contenuti all'interno dei *curricula* sono trattati per il tempo strettamente necessario per il raggiungimento delle finalità per cui sono acquisiti, fatti salvi termini di pubblicazione più lunghi previsti da disposizioni di legge.

2. In caso di procedure selettive, anche mediante affidamento diretto, il bando o l'avviso e il contratto riportano l'indicazione che il *curriculum* sarà pubblicato sul sito internet istituzionale di Ateneo.

3. I *curricula* pubblicati sono epurati dei dati non pertinenti rispetto alle finalità per cui sono stati raccolti (quali foto, data e luogo di nascita, indirizzo di residenza e di domicilio, codice fiscale, numero di telefono, e-mail personale, dati particolari e firma).

4. Nei casi di ricezione dei *curricula* spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile successivo alla ricezione dello stesso.

5. Non è dovuto il consenso al trattamento dei dati personali presenti nei *curricula* quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, nonché nei casi in cui la diffusione del *curriculum* sia prevista dalla legge.

6. Il responsabile del procedimento vigila sull'applicazione delle disposizioni del presente articolo.

Art.19 -Trattamento nell'ambito del rapporto di lavoro

1. L'Università effettua il trattamento dei dati personali nell'ambito del rapporto di lavoro, adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali, delle prerogative sindacali, e nel rispetto della legge, in particolare della Legge 20 maggio 1970, n. 300 (c.d. Statuto dei lavoratori), nonché dei contratti collettivi.

2. Il trattamento dei dati non richiede il consenso esplicito 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 nonché per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.

3. L'Università garantisce ai dipendenti il diritto di accesso ai dati valutativi di natura soggettiva.

4. L'Università può comunicare a soggetti pubblici e privati dati del personale che, in ragione di una qualità professionale specifica, usufruisce di corsi di formazione forniti in accordo con altri Enti pubblici, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.

5. I contratti riportano in apposita sezione le informazioni concernenti il trattamento dei dati personali nonché le disposizioni dell'Ateneo relative alla nomina ad autorizzati.

6. Al fine di favorire la comunicazione istituzionale, l'Università può comunicare ad altre pubbliche amministrazioni e diffondere, anche sui propri siti *web*, i nominativi del proprio personale e dei collaboratori, del ruolo ricoperto, dei recapiti telefonici e degli indirizzi telematici istituzionali.

7. L'Università può comunicare a enti pubblici e privati i dati necessari alla gestione del rapporto di lavoro, relativi al personale trasferito, comandato, distaccato o comunque assegnato in servizio a un ente diverso da quello di appartenenza.

8. Le disposizioni del presente articolo si applicano anche ai casi di collaborazione, consulenza, attività professionale e fattispecie analoghe.

Art. 20 - Diffusione dei risultati di concorsi e selezioni

1. È consentita la pubblicazione di esiti di prove concorsuali e selettive, nonché delle relative graduatorie, anche sui siti *web* di Ateneo.

2. Tale pubblicazione è effettuata nel rispetto del principio di minimizzazione e della normativa vigente in materia.

3. Nel caso di diffusione delle valutazioni sui siti *web* di Ateneo, tali informazioni sono pubblicate per un periodo di tempo non superiore a sei mesi, salvo diverse disposizioni normative in materia di Trasparenza.

Art. 21 - Trattamento dei 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

consentito, nel rispetto dei diritti e delle libertà degli interessati, se autorizzato da una norma di legge o, nei casi previsti dalla legge, da regolamento.

Art. 22 - Trattamento dei dati nelle sedute degli organi collegiali

2. Nelle sedute di tutti gli organi collegiali dell'Università il trattamento dei dati avviene in conformità al presente regolamento e al solo fine delle attività istruttorie e per le finalità deliberative di competenza degli organi.

3. La pubblicazione dei dati personali contenuti nelle deliberazioni degli organi collegiali previsti dallo Statuto è ammessa solo ove costituisca un'operazione strettamente necessaria al perseguimento delle finalità assegnate all'Ateneo da specifiche leggi o regolamenti e riguardanti informazioni utili a far conoscere ai destinatari le sue attività e il suo funzionamento o a favorire l'accesso ai servizi prestati dall'amministrazione.

Art. 23 - Trattamento dei dati per la realizzazione di video, fotografie e materiale multimediale

1. Le immagini e i dati di contatto dei soggetti coinvolti nelle riprese video, nelle fotografie e nella realizzazione di materiale multimediale rappresentano dati personali oggetto di trattamento ai sensi del presente regolamento.

2. Per la pubblicazione di video e fotografie che ritraggano persone fisiche deve essere consegnata l'informativa al trattamento dei dati personali, con richiesta del consenso al soggetto interessato e liberatoria per l'uso delle immagini ai sensi dell'art. 97 della Legge 22 aprile 1941, n. 633.

3. Il consenso, rilasciato dal genitore o dal tutore legale, è obbligatorio nel caso in cui la ripresa video o la fotografia riguardi un minore ovvero consista in un primo piano dell'interessato o in un'immagine isolata dal contesto pubblico. Resta fermo, in ogni caso, il divieto assoluto di pubblicazioni di dati di tipo sanitario.

4. 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.

5. In ogni caso il trattamento dei dati di cui al presente articolo avviene nel rispetto della dignità personale e del decoro dell'interessato.

Art. 24 - Registro delle attività di trattamento dei dati personali

1. L'Università alimenta e aggiorna il registro delle attività di trattamento, ai sensi dell'art. 30 GDPR, svolte sotto la propria responsabilità, tramite l'applicativo in uso.

2. Il registro censisce le attività di trattamento svolte da parte del Titolare del trattamento, uffici e strutture e le principali caratteristiche dei trattamenti (categoria di dati trattati; categorie di interessati; finalità del trattamento; base giuridica del trattamento; etc.). Il registro è costantemente aggiornato a cura di ciascun incaricato e, su richiesta, è messo a disposizione del Garante.

3. Il registro contiene le seguenti informazioni:

a) il nome ed i dati di contatto dell'Università, Titolare del trattamento e dell'RPD;
b) le strutture competenti al trattamento;
c) l'oggetto e le finalità del trattamento;
d) la descrizione delle categorie di interessati, nonché le categorie di dati personali;
e) le categorie di destinatari a cui i dati personali sono comunicati;
f) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
g) il periodo di conservazione;
h) le modalità di conservazione dei dati;
i) ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

4. In caso di attività di trattamento svolte dall'Università per conto di altri titolari e per i quali l'Università si configura come responsabile del trattamento, ai sensi dell'art. 28 GDPR, ogni referente sottoscrive il relativo atto di nomina, provvedendo alla tenuta e all'aggiornamento di un registro contenente le seguenti informazioni:

a) il nome e i dati di contatto di ogni titolare del trattamento per conto del quale l'Università agisce e del rispettivo responsabile della protezione dei dati nonché, ove disponibili, i riferimenti delle strutture del titolare competenti al trattamento;
b) l'oggetto e le finalità dei trattamenti effettuati per conto di ogni titolare;
c) le categorie degli interessati;
d) le categorie dei dati;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 46, par. 2, del GDPR, la documentazione delle garanzie adeguate;
f) ove possibile, il richiamo alle misure di sicurezza tecniche e organizzative adottate su istruzioni del titolare.

CAPO IV - Diritti dell'interessato e informativa

Art. 25 - Diritti dell'interessato

1. L'Università garantisce il rispetto, nonché l'esercizio dei diritti di cui agli articoli da 15 a 22 del GDPR. In particolare, l'interessato, con riferimento ai propri dati, può:

a) ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento;
b) esercitare il diritto alla limitazione del trattamento non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, o dell'accertamento dei diritti in sede giudiziaria, di tutela dei diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante;

c) esercitare il diritto di opposizione alla profilazione;
d) esercitare il diritto alla portabilità ai sensi dell'art. 20 del GDPR. Tale diritto non si applica al trattamento necessario per l'esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Università;
e) revocare in qualsiasi momento il consenso prestato senza che sia pregiudicata la liceità del trattamento fino ad allora effettuato basato sul consenso precedentemente acquisito;
f) esercitare il diritto all'oblio, chiedendo la cancellazione dei propri dati personali nel caso questi siano stati resi pubblici on-line. Tale diritto può essere esercitato ove ricorra una delle seguenti fattispecie:

- i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
- l'interessato revoca il consenso su cui si basa il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono trattati illecitamente;
- in tutti i casi previsti dalla normativa in materia.
- proporre reclamo al Garante *privacy*.

2. L'Università informa della richiesta di cancellazione ogni altro titolare e responsabile del trattamento che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione.

3. L'interessato può esercitare i suoi diritti secondo quanto previsto dalla procedura adottata dall'Università in materia di diritti dell'interessato e pubblicata sulle pagine internet dell'Università.

4. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.

5. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, l'Università può rifiutare di soddisfare la richiesta, dimostrandone il carattere manifestamente infondato o eccessivo.

Art. 26 - Informativa

1. Per ogni tipologia di trattamento dei dati, l'Università fornisce l'informativa al trattamento dei dati personali, ai sensi dell'art. 13 GDPR all'interessato, salvo il caso in cui l'interessato disponga già delle informazioni e nei casi di cui all'art. 14, par. 5, del GDPR.

2. L'informativa deve essere concisa, trasparente, intellegibile, facilmente accessibile e redatta con un linguaggio chiaro e semplice e deve contenere le seguenti informazioni:

a) i dati di contatto del titolare;
b) i dati di contatto dell'RPD;
c) le finalità e le modalità del trattamento;
d) l'indicazione dei referenti, degli eventuali sub-referenti, e i relativi dati di contatto;
e) la base giuridica del trattamento;
f) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;

g) l'eventuale volontà dell'Università di trasferire dati personali a un paese terzo (anche extra SEE) o a un'organizzazione internazionale, l'esistenza di un fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
h) il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;
i) i diritti che l'interessato può esercitare, come meglio individuati all'art. 25 del presente regolamento.
j) la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale nonchè la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
k) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.

3. Nel caso in cui i dati personali siano trattati per una finalità diversa da quella per cui sono stati raccolti, l'Università fornisce all'interessato informazioni in merito alla diversa finalità prima di tale ulteriore trattamento. Fanno eccezione a questa disposizione i trattamenti effettuati per finalità di ricerca, qualora ricorrano i presupposti individuati dall'art. 110-bis del Codice *privacy*.

4. Nel caso in cui i dati non siano raccolti presso l'interessato, l'Università si riserva la possibilità di non fornire l'informativa nel caso in cui l'interessato già disponga delle informazioni oppure comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.

5. Qualora i dati personali non siano stati ottenuti presso l'interessato, l'informativa può non essere fornita laddove si prefiguri il rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.

6. Le informative di competenza delle strutture sono redatte e aggiornate dai referenti, secondo lo schema tipo anche con il supporto del RPD.

7. La modulistica, sia cartacea che digitale, che prevede la raccolta di dati riferiti a una persona fisica, deve contenere il riferimento all'informativa specifica.

8. I soggetti autorizzati e i responsabili esterni che operano per conto dell'Università trattano i dati personali solo per le specifiche finalità indicate nell'informativa fornita all'interessato al momento del conferimento dei dati e per ogni altra finalità prevista dalla legge.

Art. 27 - Comunicazione e diffusione dei dati personali

1. La comunicazione e la diffusione dei dati personali, diversi da quelli particolari e giudiziari, sono permesse quando:

a) siano previste da norme di legge, di regolamento o dal diritto dell'Unione europea;
b) siano necessarie per finalità di ricerca scientifica o di statistica e i dati siano trattati in forma anonima o aggregata;
c) siano richieste per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o

repressione di reati, con l'osservanza delle norme che regolano la materia.

2. La comunicazione di dati a soggetti pubblici è sempre ammessa per i fini istituzionali e, ove prevista, da norma di legge o regolamento.

3. Ove ricorrano i requisiti di cui ai commi precedenti, le richieste da parte di soggetti privati ed enti pubblici economici volte a ottenere la comunicazione di dati, devono essere formulate per iscritto e motivate, con l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti.

4. Il titolare, per il tramite dei referenti, valuta la legittimazione del richiedente a ottenere tali dati e ove sia positiva, autorizza la visione o la trasmissione dei dati nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.

CAPO V - Misure di sicurezza, violazione dei dati e sanzioni

Art. 28 – Sicurezza

1. Al fine di garantire la sicurezza dei dati, il titolare del trattamento adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio connesso al trattamento. Tali misure sono finalizzate a ridurre al minimo, in particolare, il rischio di distruzione, perdita, modifica, divulgazione non autorizzata, accesso in modo accidentale o illegale, ai dati personali trattati.

2. I referenti del trattamento adottano le misure di cui al comma 1 sulla base delle istruzioni fornite dal titolare, che tengono conto delle risorse finanziarie, tecniche e umane disponibili.

3. L'Università, per il tramite del proprio centro servizi informatici o di altra struttura a tal fine individuata, effettua la valutazione dei rischi connessi al trattamento e adotta misure di sicurezza comprendenti, tra le altre:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
e) l'obbligo di adottare le misure di sicurezza previste da codici di condotta di settore, ove esistenti, e dalle certificazioni, ove acquisite (artt. 40 - 43 GDPR).

4. Le misure di sicurezza sono riesaminate in modo periodico, pubblicate sulla rete intranet e illustrate nelle sessioni formative.

5. Solo in circostanze eccezionali i dati personali possono essere trasferiti fuori dagli ambienti dell'Università e sotto la diretta responsabilità di personale autorizzato. In particolare, il personale

autorizzato è tenuto a:

a) ove possibile, fare uso di accesso remoto alle informazioni tramite *login* e *password*;
b) trasportare solo la quantità minima di dati personali;
c) assicurarsi che i dispositivi mobili e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali fuori dagli ambienti universitari siano dotati di sistemi di crittografia.

6. Qualunque perdita e/o furto di dati deve essere tempestivamente segnalato e trattato secondo la procedura di gestione delle violazioni di dati personali –*data breach*, predisposta dall'Università.

Art. 29 - La valutazione di impatto

1. L'RPD procede annualmente o a seguito di sopravvenuti cambiamenti normativi o organizzativi all'individuazione o alla rivalutazione dei parametri attraverso i quali viene effettuata la valutazione di impatto.

2. Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità nonché l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare, per tramite dei referenti, previa consultazione con l'RPD e con i Servizi Informatici o altra struttura a tal fine individuata, effettua, prima di procedere al trattamento, la valutazione d'impatto sulla protezione dei dati personali (DPIA).

3. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.

4. La valutazione d'impatto sulla protezione dei dati è obbligatoria nei seguenti casi:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente sulle persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali quali: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza);
d) in tutti gli altri casi in cui la normativa o il Garante per la protezione dei dati personali lo prevedano.

5. Il referente può consultare l'RPD e richiedere un parere in merito alla decisione di effettuare o meno la valutazione di impatto. Il parere dell'RPD è conservato a cura del referente. Qualora il referente adotti con provvedimento motivato condotte difformi da quelle indicate, questi è tenuto a darne comunicazione al RPD.

6. Il responsabile per la transizione al digitale fornisce supporto ai referenti e collabora con l'RPD ai fini dello svolgimento della valutazione di impatto, anche con compiti di vigilanza.

7. In caso di modifiche del trattamento, in particolare quando insorgono variazioni del rischio, il referente

procede a un riesame per valutare se esso sia effettuato conformemente alla valutazione di impatto sulla protezione dei dati e, se necessario, procede a una revisione della medesima.

Art. 30 - Videosorveglianza

1. I sistemi di videosorveglianza possono essere installati per garantire la sicurezza e l'incolumità del personale dipendente, degli studenti e dei frequentatori a vario titolo degli spazi universitari, nonché allo scopo di tutelare il patrimonio dell'Ateneo da atti vandalici, danneggiamenti e furti, prevenendo e perseguendo il compimento di eventuali atti illeciti.

2. Il trattamento dei dati personali effettuato mediante l'attivazione di impianti di videosorveglianza negli ambienti dell'Università si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.

3. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate dall'Ateneo e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria.

4. L'Università garantisce la riservatezza, la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza. In particolare:

a) solo il personale autorizzato e formato o istruito può avere accesso alle immagini;
b) il personale autorizzato è tenuto al segreto professionale.

5. Qualora il sistema di videosorveglianza preveda la registrazione delle immagini, le stesse possono essere conservate per un periodo non superiore alle 72 ore dalla ripresa. Nel caso di sospetta o evidente notizia di danno o di reato, le immagini possono essere estrapolate su espressa richiesta dell'autorità giudiziaria o del soggetto che abbia sporto denuncia/querela. Decorsi i termini di conservazione previsti dai regolamenti o dalle procedure interne, le immagini devono essere cancellate a cura dell'autorizzato in modo irreversibile rendendo non riutilizzabili i dati cancellati.

6. È onere dell'ufficio preposto al trattamento dei dati personali della struttura nella quale sono installati strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio:

a) adottare le garanzie di cui all'art. 4 della legge del 20 maggio 1970, n. 300, non potendosi configurare la predisposizione del sistema di videosorveglianza quale controllo a distanza del personale dipendente;
b) garantire l'osservanza dei principi di necessità, finalità e proporzionalità del trattamento dei dati;
c) garantire il rispetto del presente regolamento, delle prescrizioni imposte dal Garante *privacy* e dalla normativa vigente, anche in relazione all'utilizzo di particolari tecnologie e/o apparecchiature.

7. Qualora vengano installate apparecchiature di videosorveglianza in ambienti e zone accessibili al pubblico, la valutazione di impatto è effettuata nei casi previsti dalla legge.

Art. 31 - Sanzioni disciplinari e amministrative

1. Fermo restando quanto previsto dagli artt. 58, 82, 83 e 84 del GDPR e dal Codice *privacy,* le sanzioni disciplinari e amministrative a carico del personale in caso di violazione delle leggi, del presente regolamento e delle procedure in tema di protezione dei dati personali saranno definite dall'Università anche sulla base di quanto disposto dai CCNL, dal Codice Etico e dal Codice di Comportamento dei dipendenti dell'Università degli Studi di Brescia.

CAPO VI - Disposizioni finali

Art. 32 - Disposizioni finali ed entrata in vigore

1. Per quanto non espressamente previsto dal presente regolamento si rinvia alle disposizioni del GDPR e del Codice *privacy*, oltre che a quanto previsto dalle Linee guida, dai provvedimenti e regole deontologiche adottate e approvate dal Garante *privacy*.

2. Il presente regolamento, approvato dall'organo competente, è emanato con decreto del Rettore ed è pubblicato nell'albo on-line dell'Ateneo, nonché sul relativo sito istituzionale. Esso entra in vigore il primo giorno feriale successivo alla pubblicazione all'albo on-line di Ateneo.