UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

Regolamento in materia di protezione dei dati personali

Parere del Consiglio di Amministrazione del 16.12.2022

Approvato dal Senato Accademico del 21.02.2023

Art. 1 – Ambito di applicazione

1. Adottato in attuazione del Regolamento (UE) 27 aprile 2016, n. 679 ("*Regolamento Generale sulla Protezione dei Dati*", di seguito GDPR) e del D. Lgs. 30 giugno 2003, n.196 e ss.mm.ii. ("*Codice in materia di protezione dei dati personali*", di seguito Codice privacy) e in particolare l'art. 2-quaterdecies del Codice privacy, il presente Regolamento disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali effettuato dall'Università degli Studi di Udine (di seguito Università) in qualità di Titolare, Contitolare o Responsabile esterno.

2. È un dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

3. Sono dati particolari l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

4. L'Università provvede al trattamento, alla comunicazione e alla diffusione dei dati personali nel perseguimento dei propri fini istituzionali, nei limiti stabiliti dalle leggi e dalle altre disposizioni generali, dallo Statuto, dal presente Regolamento e dai provvedimenti emanati dal Garante per la protezione dei dati personali (di seguito Garante).

5. L'Università, in qualità di Titolare, effettua i trattamenti di dati con o senza ausilio di strumenti informatici.

6. L'Università pone in essere un trattamento lecito, corretto e trasparente dei dati personali, al fine di instaurare e mantenere un rapporto di fiducia con la comunità universitaria e i terzi interessati.

7. Tutti coloro che trattano dati personali di cui l'Università è Titolare, Contitolare o Responsabile, effettuano il trattamento secondo la normativa europea e italiana, la disciplina interna stabilita dal presente Regolamento nonché in base all'incarico o alla nomina specificamente ricevuti.

Art. 2 – Ruoli del sistema di trattamento dei dati

1. All'interno dell'organizzazione dell'Università sono individuati, con specifici atti, le responsabilità ed i mezzi attraverso i quali viene veicolata l'informazione riguardante il corretto trattamento dei dati personali, per permettere l'esecuzione efficace ed efficiente delle procedure nell'ambito della protezione dei dati, rendendo possibili le funzioni del Titolare del trattamento.

2. A tal fine, si delineano due diverse configurazioni organizzative: una struttura verticale ed una struttura orizzontale. La prima individua gli attori che hanno il compito di gestire e proteggere il dato relativo alla struttura di appartenenza (Responsabile interno, delegati, autorizzati) e ne descrive le funzioni. La seconda, con carattere di trasversalità, individua le figure preposte ad informare e vigilare gli attori della struttura verticale sulla corretta gestione dei trattamenti dei dati (Responsabile della Protezione dei Dati e Gruppo di lavoro a supporto del Responsabile della Protezione dei Dati).

Art. 3 – Il responsabile della protezione dei dati personali (RPD)

1. In ossequio all'art. 37 GDPR, l'Università nomina, con decreto del Rettore, un Responsabile della Protezione dei Dati (di seguito RPD).

2. L'Università garantisce che il RPD eserciti le proprie funzioni nel rispetto di quanto stabilito dall'art. 38 GDPR.

3. L'Università nomina a supporto del RPD:

a) il Gruppo di lavoro a supporto del Responsabile della Protezione dei Dati (di seguito Gruppo di lavoro)
b) una rete di responsabili interni, che operano, nell'ambito delle strutture nelle quali i dati personali sono trattati, per le finalità istituzionali e sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.

4. Su indicazione del RPD e del Gruppo di lavoro possono essere costituiti specifici gruppi di lavoro.

5. Sull'attività svolta il RPD redige una relazione annuale che viene comunicata al Rettore e al Direttore Generale.

Art. 4 – Responsabili esterni del trattamento dei dati personali

1. É Responsabile esterno del trattamento qualunque persona fisica o giuridica che effettua trattamenti di dati personali per conto dell'Università ai sensi dell'art. 28 GDPR.

2. I Responsabili esterni del trattamento sono nominati con apposito atto del Rettore contenente le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste dal GDPR. I Direttori di dipartimento nominano i responsabili esterni per i trattamenti dati concernenti le loro strutture. In caso di trattamenti dati concernenti più Dipartimenti, la nomina spetta congiuntamente ai relativi Direttori.

3. Il Titolare può delegare la nomina di responsabili esterni o, anche disgiuntamente dalla nomina, l'eventuale successiva determinazione o precisazione delle relative istruzioni.

Art. 5 – Contitolarità del trattamento dei dati personali

1. Vi è contitolarità del trattamento laddove due o più titolari del trattamento determinino congiuntamente le finalità e i mezzi del trattamento, ai sensi dell'art. 26 GDPR.

2. Essi determinano in modo trasparente, mediante un Accordo, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa, i propri ruoli e i rapporti con gli interessati.

3. Il Titolare può delegare la sottoscrizione degli accordi di contitolarità.

Art. 6 – Responsabili interni del trattamento dei dati personali

1. Sono qualificati Responsabili interni del trattamento dei dati personali, sulla base della funzione svolta nell'ambito delle rispettive strutture, i seguenti soggetti:

a) il responsabile d'ufficio di primo livello, per l'amministrazione centrale;
b) i responsabili dei servizi dipartimentali, per i dipartimenti.

2. Sono qualificati Responsabili interni del trattamento dei dati personali, sulla base della funzione svolta, ad esclusione dei dati relativi alla mera gestione amministrativa, i seguenti soggetti:

a) il docente di riferimento, dipendente o incaricato esterno di insegnamento, per il trattamento relativo ai dati personali inerenti all'attività didattica;
b) il docente di riferimento, per il trattamento relativo ai dati personali contenuti negli elaborati prodotti dagli studenti nell'ambito della loro carriera universitaria o in relazione al conseguimento del titolo finale (es. laurea, dottorato, master);
c) il *Principal investigator,* responsabile scientifico o analoga posizione, per il trattamento effettuato anche dai collaboratori nell'ambito di progetti o attività di ricerca, compresa la ricerca libera;
d) il docente referente del contratto o della convenzione attinenti ad attività di ricerca, di didattica o di terza missione, per il trattamento dei dati personali inerenti tali rapporti.

3. I Responsabili interni di cui al comma 1, adeguatamente formati riguardo alle implicazioni della loro attività rispetto alla protezione dei dati personali, nell'ambito delle loro competenze, operano per l'adempimento dei seguenti compiti:

a) vigilare, monitorare e garantire il rispetto di quanto previsto dalle norme vigenti in materia;
b) rispettare ed applicare le disposizioni previste dalla disciplina d'Ateneo;
c) collaborare con il Gruppo di lavoro al miglioramento delle procedure interne e all'aggiornamento della documentazione;
d) collaborare, per la parte di propria competenza, alla mappatura dei trattamenti, al censimento delle banche dati e dei trattamenti di dati esternalizzati e alla implementazione e aggiornamento del registro dei trattamenti;
e) curare la predisposizione, sulla base di modelli messi a disposizione dall'Ateneo, e l'aggiornamento della modulistica (es. informativa privacy) per i trattamenti di competenza, avvalendosi, se del caso, dell'appoggio del Gruppo di lavoro;
f) impartire o assicurarsi che vengano impartite idonee istruzioni in materia di informativa privacy e di misure di sicurezza al personale autorizzato al trattamento;
g) vigilare sul rispetto delle misure di sicurezza finalizzate ad evitare i rischi, anche accidentali, di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
h) collaborare alla determinazione della valutazione d'impatto privacy ex art. 35 GDPR per i trattamenti di propria competenza;
i) relativamente ai trattamenti di propria competenza, comunicare prontamente le violazioni di dati personali (*Data Breach*) e le richieste di esercizio dei diritti di cui agli artt. 15 – 22 GDPR;
j) partecipare obbligatoriamente alle sessioni informative/formative e di sensibilizzazione in materia di protezione dei dati personali;
k) decidere sulle richieste di condivisione da parte di utenti interni nel caso di diniego opposto dai propri autorizzati e nel caso di richieste di condivisione dei dati di cui all'art. 8, comma 4 del presente Regolamento;
l) valutare eventuali richieste, da parte di soggetti privati, relative alla comunicazione o diffusione di dati personali;
m) collaborare con l'ufficio preposto per individuare i bisogni formativi delle risorse della propria struttura;
n) per i trattamenti che hanno come base giuridica il consenso, predisporre le misure organizzative atte a condizionare i trattamenti secondo il consenso ottenuto e a garantire la raccolta e la conservazione del consenso o della sua eventuale revoca, siano essi espressi in forma cartacea o elettronica, nonché a dare seguito alle operazioni relative alla revoca del consenso.

4. I Responsabili interni di cui al comma 2, adeguatamente formati riguardo alle implicazioni della loro attività rispetto alla protezione dei dati personali, operano nell'ambito delle competenze loro affidate per l'adempimento dei seguenti compiti:

a) vigilare, monitorare e garantire il rispetto di quanto previsto dalle norme vigenti in materia;
b) rispettare ed applicare le disposizioni previste dalla disciplina d'Ateneo;
c) collaborare con il Gruppo di lavoro al miglioramento delle procedure interne e all'aggiornamento della documentazione;
d) curare la compilazione della modulistica (es. informativa privacy, scheda GDPR progetti di ricerca) per i trattamenti di competenza, avvalendosi, se del caso, dell'appoggio del Gruppo di lavoro;
e) impartire o assicurarsi che vengano impartite idonee istruzioni in materia di informativa privacy e di misure di sicurezza al personale autorizzato al trattamento;
f) vigilare sul rispetto delle misure di sicurezza finalizzate ad evitare i rischi, anche accidentali, di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
g) collaborare alla determinazione della valutazione d'impatto privacy ex art. 35 GDPR per i trattamenti di propria competenza;
h) relativamente ai trattamenti di propria competenza, comunicare prontamente le violazioni di dati personali (*Data Breach*) e le richieste di esercizio dei diritti di cui agli artt. 15 – 22 GDPR;
i) partecipare obbligatoriamente alle sessioni informative/formative e di sensibilizzazione in materia di protezione dei dati personali.

5. Il Responsabile interno di cui al comma 1 può delegare a uno o più soggetti competenti, dipendenti dell'Università, in tutto o in parte lo svolgimento dei compiti di cui al comma 3, fatta eccezione per quanto indicato alle lettere c), h), i), j), k), l). Con riferimento alla lettera e), l'avvalersi dell'appoggio del Gruppo di lavoro non può essere delegato.

Il Responsabile interno di cui al comma 2 può delegare a uno o più soggetti competenti, dipendenti/interni dell'Università, in tutto o in parte lo svolgimento dei compiti di cui al comma 4, fatta eccezione per quanto indicato alle lettere c), g), h), i). Con riferimento alla lettera d), l'avvalersi dell'appoggio del Gruppo di lavoro non può essere delegato.

6. La delega è documentata con apposita comunicazione che contiene puntualmente i compiti delegati ed è corredata dalle relative istruzioni sintetiche e dalla individuazione delle modalità di verifica e di controllo. Essa è inoltrata al Gruppo di lavoro.

7. I responsabili interni hanno il dovere di conservare e aggiornare l'elenco dei soggetti delegati e verificare periodicamente i contenuti della delega.

Art. 7 – Autorizzati al trattamento

1. Gli autorizzati al trattamento sono le persone fisiche che, per lo svolgimento delle attività di competenza o per l'adempimento dei compiti propri della struttura cui afferiscono, appartengono, dipendono o a cui sono aggregati trattano effettivamente dati personali.

2. Gli autorizzati al trattamento ricevono formazione/informazione in materia di trattamento dei dati personali.

3. L'autorizzato effettua i trattamenti dei dati personali in osservanza delle misure di sicurezza previste dall'Università finalizzate ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati personali.

4. L'autorizzato è tenuto:

a) a mantenere confidenziali tutte le informazioni di cui sia venuto a conoscenza in occasione dell'attività prestata, anche dopo la cessazione del suo rapporto con l'Università;
b) a non comunicare a terzi o diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di autorizzato;
c) a partecipare alle occasioni d'informazione e formazione in materia di protezione dei dati personali e a sostenere gli eventuali test finali per la verifica dell'apprendimento;
d) a segnalare con tempestività al Responsabile interno competente e al delegato eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante e ai soggetti interessati ("*Data Breach*").

5. L'autorizzato è informato che l'accesso e la permanenza nei sistemi informativi aziendali per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informativi (art. 615-ter c.p.) e può comportare l'irrogazione di sanzioni disciplinari, oltre che il risarcimento dell'eventuale danno causato a terzi e all'Università.

6. I soggetti terzi rispetto all'Università non sono legittimati ad accedere a dati personali a meno che non siano stati nominati responsabili esterni o siano contitolari del trattamento, fatte salve le ipotesi di accesso documentale o civico in quanto applicabili.

Art. 8 – Condivisione dei dati personali all'interno dell'università

1. Il trattamento e la condivisione dei dati personali trattati dall'Università sono conformi ai principi della confidenzialità e dell'efficienza amministrativa e sono sempre fondati su di una base giuridica.

2. Chi richiede un dato personale ne motiva le ragioni. La giustificazione può anche essere esposta sinteticamente, purché sia comprensibile.

3. In caso di rifiuto di condivisione del dato personale da parte dell'autorizzato, il richiedente può rivolgersi al Responsabile interno competente.

4. Il Responsabile interno decide sempre in merito alla condivisione delle seguenti tipologie di dati personali:

a) dati particolari ai sensi dell'art. 9 GDPR;
b) dati relativi a procedimenti disciplinari o giudiziari;
c) dati inerenti la situazione reddituale o patrimoniale;
d) dati concernenti la valutazione della produttività personale.

In caso di rifiuto da parte del Responsabile interno, il richiedente può rivolgersi al Responsabile della Protezione dei Dati.

5. La condivisione del dato personale in assenza di base giuridica comporta la responsabilità sia del richiedente sia del conferente. La condivisione del dato personale in violazione delle disposizioni del presente articolo comporta la responsabilità del conferente.

Art. 9 – Formazione e informazione

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, l'Università sostiene e promuove, all'interno delle proprie strutture, ogni strumento di informazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo l'Università promuove l'attività formativa del proprio personale.

2. L'Università aggiorna periodicamente, sentito il RPD e il Gruppo di lavoro, un piano formativo specifico in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata. Tale formazione, sentito il Responsabile della Prevenzione della Corruzione e della Trasparenza, è integrata e coordinata con la formazione in materia di prevenzione della corruzione, nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'Università.

3. La frequenza delle attività di formazione è obbligatoria e viene considerata quale elemento di valutazione della performance.

Art. 10 – Diritti dell'interessato

1. L'Università garantisce il rispetto e l'esercizio dei diritti degli interessati di cui agli artt. da 15 a 22 GDPR.

2. L'interessato può esercitare i suoi diritti con richiesta scritta indirizzata all'amministrazione (datipersonali@uniud.it). Il Responsabile interno competente per la gestione dei dati personali oggetto della richiesta può consultare il Gruppo di lavoro nell'evasione delle richieste degli interessati che presentano particolari criticità.

3. Il riscontro alla richiesta presentata dall'interessato viene fornito dall'Università per mezzo del Responsabile interno competente per i dati di che trattasi, senza ingiustificato ritardo entro 30 giorni dalla data della richiesta, anche nei casi di diniego. Per i casi di particolare e comprovata difficoltà il termine dei 30 giorni può essere esteso fino a 3 mesi, non ulteriormente prorogabili. Di tale proroga viene data informazione all'interessato entro 30 giorni dalla data della richiesta.

4. Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.

5. L'esercizio dei diritti è, di norma, gratuito per l'interessato. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, l'Università può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi sostenuti oppure può rifiutare di soddisfare la richiesta, dimostrando il carattere manifestamente infondato o eccessivo della richiesta.

Art. 11 – Trattamento di categorie particolari di dati personali e dati personali relativi a condanne penali e reati

1. I dati particolari possono essere oggetto di trattamento in presenza di una delle condizioni di cui all'art. 9, par. 2 GDPR ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dagli artt. 2-sexies e 2-septies del Codice privacy.

2. Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito unicamente nei casi previsti dall'art. 2-octies del Codice privacy.

Art. 12 – Accesso ai documenti amministrativi e accesso civico

1. I limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e per l'esercizio dell'accesso civico sono disciplinati rispettivamente dalla legge 7 agosto 1990, n. 241, dal decreto legislativo 14 marzo 2013, n. 33, nonché dagli artt. 59 e 60 del Codice privacy.

Art. 13 – Comunicazione o diffusione dei dati personali

1. La comunicazione o la diffusione dei dati personali, esclusi i dati di cui all'art.11 è consentita quando:

a) sia prevista da norme di legge, di regolamento o dal diritto dell'Unione europea;
b) sia necessaria per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o aggregati;
c) sia richiesta 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 personali è ammessa nei casi di cui all'art. 2-ter del Codice Privacy.

3. Fermo restando quanto disposto dal successivo comma 7, l'Università, tramite i Responsabili interni, con il supporto del Gruppo di lavoro, valuta, sulla base delle norme vigenti e di quanto previsto dal presente Regolamento, eventuali richieste di comunicazione o diffusione di dati personali a soggetti privati, decidendo se e come dare seguito alla richiesta.

4. Le modalità di comunicazione dei predetti dati, per le quali può essere richiesto un contributo a copertura dei costi sostenuti, sono decise dall'Università.

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

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

7. L'Università, al fine di agevolare l'orientamento, le esperienze formative e professionali e l'eventuale collocazione nel mondo del lavoro, anche all'estero, può comunicare o diffondere, anche su richiesta di soggetti privati e per via telematica, dati ed elenchi riguardanti coloro che hanno intrapreso, terminato o concluso, a qualsiasi titolo, un percorso formativo o di ricerca presso l'Ateneo. La finalità deve essere dichiarata nella richiesta e i dati potranno essere utilizzati per le sole finalità per le quali sono stati comunicati o diffusi.

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

9. In considerazione del sistema di autovalutazione, accreditamento e valutazione periodica dei corsi di studio definito dal MUR, l'Università può elaborare e/o comunicare le opinioni degli studenti sulla didattica agli organismi deputati ad effettuare verifiche della qualità della didattica. Tali dati sono trattati con lo scopo di definire azioni volte al miglioramento della qualità della didattica.

10. L'Università può comunicare, alle Aziende Ospedaliere in convenzione, dati inerenti al personale dell'Università che eserciti la propria attività nell'ambito della convenzione con tali Enti.

Art. 14 – Trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

1. Il trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è effettuato in conformità all'art. 89 GDPR e a quanto disposto dal Codice privacy, dalla normativa di settore e dalle regole deontologiche in materia approvate dal Garante.

2. Laddove lo svolgimento di una ricerca scientifica o storica o a fini statistici comporti il trattamento di dati personali, si rende necessaria la redazione di apposita documentazione, richiesta dal Garante, il cui modello, predisposto dall'Università, è reso disponibile attraverso i canali dedicati.

3. Coloro i quali effettuano l'attività di ricerca si impegnano a conformarsi alla normativa in materia di protezione dati personali e alle regole deontologiche emanate dal Garante. Il Responsabile interno di cui all'art. 6, comma 2 adotta le misure di cui all'art. 6, comma 4.

4. Nei casi previsti dai rispettivi Dipartimenti, il trattamento dei dati personali per finalità di ricerca deve avvenire conformemente a quanto previsto dai competenti Comitati Etici.

Art. 15 – Diffusione delle valutazioni d'esame

1. In ottemperanza ai principi di trasparenza cui l'Università si ispira e 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* dell'Università.

2. La pubblicazione dei dati sul sito *web* o attraverso altre modalità di comunicazione è consentita unicamente mediante la diffusione del numero di matricola dello studente e del voto o della valutazione conseguiti.

3. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a tre mesi.

Art. 16 – Diffusione dei risultati di concorsi e selezioni

1. In ottemperanza ai principi di trasparenza cui l'Università si ispira e alla normativa in materia, è consentita la pubblicazione di esiti di prove concorsuali e selettive, nonché delle relative graduatorie, anche sul sito *web* dell'Università.

2. La pubblicazione dei dati sul sito *web* è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati.

3. Nel caso di diffusione delle valutazioni sul sito *web*, tali informazioni sono pubblicate per un periodo di tempo non superiore a sei mesi, salvi i casi nei quali la legge o i regolamenti dispongano un periodo maggiore.

Art. 17 – Sicurezza

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

2. Nel valutare l'adeguato livello di sicurezza, l'Università tiene conto dei rischi che derivano in particolare dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, dalla modifica, dalla distruzione, dalla perdita dei dati personali trasmessi, conservati o comunque trattati, nonché i rischi intrinseci che il trattamento di alcune tipologie di dati personali può comportare.

3. Qualunque perdita e/o furto di dati deve essere tempestivamente segnalato e trattato secondo la procedura di gestione delle violazioni di dati personali di cui al successivo art. 20.

Art. 18 – Registro della attività di trattamento

1. L'Università istituisce un Registro delle attività di trattamento svolte sotto la propria responsabilità, aggiornato periodicamente dai Responsabili interni e loro delegati, come previsto dal presente Regolamento.

2. Il Registro censisce le attività di trattamento svolte dagli uffici e dalle altre strutture dell'Università e le principali caratteristiche dei trattamenti. Il registro è, su richiesta, messo a disposizione del Garante.

3. Nel Registro sono elencati e descritti sia i trattamenti dei quali l'Università è Titolare sia i trattamenti che l'Università effettua in qualità di Responsabile esterno di altri titolari.

Art. 19 – La valutazione di impatto privacy

1. Quando si rende necessaria una valutazione d'impatto (*Data Protection Impact Assessment*) sulla protezione dei dati ai sensi dell'art. 35 GDPR, il RPD e il Gruppo di lavoro, se richiesto, forniscono un parere preliminare e ne sorvegliano lo svolgimento. La valutazione d'impatto da effettuarsi è sempre comunicata al RPD dopo il suo svolgimento.

2. L'Università, per il tramite del RPD, consulta il Garante prima di procedere al trattamento se le risultanze della valutazione di impatto (*Data Protection Impact Assessment*) indicano l'esistenza di un rischio residuale elevato.

Art. 20 – Violazione di dati personali (*Data Breach*)

1. Al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati, l'Università in qualità di Titolare del trattamento definisce una procedura di gestione delle violazioni di dati personali.

2. Tale procedura si applica a qualunque attività di trattamento svolta all'interno della struttura organizzativa del Titolare.

3. La procedura definisce le modalità per identificare la violazione, analizzare le cause della violazione, definire le misure da adottare per rimediare alla violazione dei dati personali, attenuarne i possibili effetti negativi, registrare le informazioni relative alla violazione, identificare le azioni correttive e valutarne l'efficacia, notificare la violazione di dati personali al Garante nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche, comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio sia elevato.

4. La procedura è approvata mediante specifico provvedimento del Direttore Generale.

5. La procedura costituisce una delle materie oggetto della formazione del personale di cui all'art. 9.

6. Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa può comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

Art. 21 – Videosorveglianza

1. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate in materia di videosorveglianza e non possono essere diffusi o comunicati a terzi, salvo i casi previsti dalla legge.

2. L'Università garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza, come da apposita procedura. In particolare:

- solo il personale autorizzato può avere accesso alle immagini;
- il personale autorizzato è tenuto al segreto professionale;
- le immagini non possono essere conservate per un periodo più lungo del necessario in conformità con quanto previsto dai principi applicabili al trattamento dei dati personali;
- nel caso in cui le immagini siano conservate per un periodo maggiore di quello previsto, esse devono essere custodite in un posto sicuro con accesso controllato e cancellate non appena la loro conservazione non sia più necessaria.

3. Ai fini del rispetto della protezione dei dati personali, è necessario che la videosorveglianza si svolga in modo da:

~~a)~~ adottare le garanzie di cui all'art. 4 della legge del 20 maggio 1970, n. 300 (Statuto dei lavoratori);
b) redigere un documento in cui siano riportate le ragioni dell'installazione di tali sistemi anche ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso.

4. Resta ferma la necessità di effettuare una valutazione di impatto (DPIA) ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.

Art. 22 – Disposizioni finali

1. Il presente Regolamento è emanato con Decreto del Rettore.

2. Dalla data di entrata in vigore del presente Regolamento, devono intendersi abrogate tutte le norme regolamentari incompatibili in relazione a soggetti e materie interessate al trattamento, in particolare le disposizioni contenute nel Regolamento emanato con D.R. n. 150 del 23.02.2005 (Riservatezza dati personali).

3. Dove non diversamente previsto l'attuazione del presente Regolamento è demandata a provvedimenti o regolamenti attuativi del Rettore e/o del Direttore Generale.

Art. 23 – Efficacia temporale e pubblicità

1. Il presente Regolamento entra in vigore il giorno successivo alla sua emanazione.

2. L'Università provvede a dare pubblicità al presente Regolamento e alle successive modifiche ed integrazioni mediante pubblicazione sul sito *web* d'Ateneo.