UNIVERSITÀ DEL PIEMONTE ORIENTALE

DIREZIONE GENERALE

Staff Servizi Legali di Ateneo

Via Duomo, 6 – 13100 Vercelli VC
Tel. 0161 261533
E-mail: affarigiuridici@uniupo.it
PEC protocollo@pec.uniupo.it

LS/ff

OGGETTO: Aggiornamento del Regolamento di Ateneo per l'attuazione delle norme in materia di protezione dei dati personali (Regolamento UE 2016/679 "GDPR"- D.Lgs 196/2003 come emendato dal D.Lgs 101/2018).

IL RETTORE

VISTO lo Statuto di Ateneo, emanato con D.R. rep. n. 444 del 14.11.2001 e modificato con D.R. rep. n. 300/2014 del27.05.2014;
VISTO il Regolamento Generale di Ateneo, emanato con D.R. rep. n237/2014 del 16.04.2014;
VISTO il Regolamento di Ateneo per l'attuazione delle norme in materia di dati personali emanato con Decreto Rettorale Rep. n. 471/2015 del 06.07.2015;
CONSIDERATO che a partire dal 2018 la disciplina in materia di protezione dei dati personali ha subito numerosi aggiornamenti e modifiche, la più importante delle quali coincide con la piena applicabilità del Regolamento UE 2016/679 (GDPR);
CONSIDERATO che con il GDPR vengono introdotte le seguenti novità:

- si introduce il concetto di responsabilizzazione o accountability del titolare;
- si introducono importi più elevati per le sanzioni amministrative pecuniarie che variano nel massimo a seconda delle disposizioni violate;
- si introducono concetti di "privacy by design", nonché di approccio basato sul rischio e adeguatezza delle misure di sicurezza, di valutazione d'impatto e data breach;
- regole più rigorose per la selezione e la nomina di un responsabile del trattamento e di eventuali sub-responsabili;
- si introduce la previsione in alcuni casi tassativi di nomina obbligatoria di un Responsabile della protezione dei dati;
- si introducono regole più chiare su informativa e consenso;
- viene ampliata la categoria dei diritti che spettano all'interessato;
- vengono stabiliti criteri rigorosi per il trasferimento degli stessi al di fuori dell'UE;

CONSIDERATO che in data 19 settembre 2018 è entrato in vigore il D.Lgs. 10 agosto 2018, n. 101 recante disposizioni per l'adeguamento del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) alle disposizioni del GDPR;
CONSIDERATO che in questi anni l'Autorità Garante per la protezione dei dati personali ha emesso linee guida e provvedimenti relativi all'applicazione del GDPR;
CONSIDERATO che il Comitato Europeo per la protezione dei dati personali ("EDPB", ex Gruppo di lavoro Art. 29) ha emesso provvedimenti per assicurare che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia;

CONSIDERATO che alla luce delle disposizioni normative vigenti, lo Staff Servizi Legali di Ateneo con il supporto del DPO ha avviato un'attività di analisi dei contenuti del regolamento di Ateneo e ha apportato le seguenti modifiche al testo regolamentare:

- aggiornamento della categoria dei dati sensibili;
- disciplina della figura del DPO, del referente interno, del responsabile del trattamento e del soggetto autorizzato al trattamento;
- disciplina dell'accesso ai dati prevedendone, in linea generale, la gratuità;
- disciplina dell'informativa;
- disciplina della valutazione d'impatto sulla protezione dei dati (DPIA) e della consultazione preventiva;
- previsione di adeguate misure di sicurezza e analisi dei rischi;

VISTA la deliberazione n. 7/2023/6.1, con la quale il Consiglio di Amministrazione, nel corso della seduta del 23.05.2023, ha espresso, ai sensi dell'art. 13, lettera t, dello Statuto vigente, parere favorevole sul nuovo testo del regolamento di Ateneo per l'attuazione delle norme in materia di protezione dei dati personali;

VISTA la deliberazione n. 8/2023/6.1, con la quale il Senato Accademico ha approvato ai sensi dell'art. 12, comma 2, lettera f, dello Statuto vigente, il nuovo testo del regolamento di Ateneo per l'attuazione delle norme in materia di protezione dei dati personali (Regolamento UE 2016/679 "GDPR" - D.Lgs 196/2003 come emendato dal D.Lgs 101/2018);

VALUTATO ogni opportuno elemento

DECRETA

1. È emanato il nuovo testo del regolamento di Ateneo per l'attuazione delle norme in materia di protezione dei dati personali (Regolamento UE 2016/679 "GDPR" - D.Lgs 196/2003 come emendato dal D.Lgs 101/2018), allegato al presente decreto (All. A).

2. Il presente Regolamento entra in vigore il giorno dopo la sua emanazione ed è pubblicato all'albo e sul sito web dell'Università.

Visto
La Direttrice Generale
(Dott.ssa Loredana Segreto)

Il Rettore
(Prof. Gian Carlo Avanzi)

Documento informatico sottoscritto con firma digitale ai sensi del D.Lgs. n. 82/2005 e ss.mm.ii

Allegato A

REGOLAMENTO DI ATENEO PER L'ATTUAZIONE DELLE NORME IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (REGOLAMENTO UE 2016/679 "GDPR - D.LGS 196/2003 COME EMENDATO DAL D.LGS 101/2018)

REGOLAMENTO DI ATENEO PER L'ATTUAZIONE DELLE NORME IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (REGOLAMENTO UE 2016/679 "GDPR" - D.LGS 196/2003 COME EMENDATO DAL D.LGS 101/2018)

PARTE I
DISPOSIZIONI GENERALI

Articolo 1 – Ambito di applicazione

1. Il presente Regolamento è emanato in attuazione delle Leggi in materia di protezione dei dati personali e disciplina il trattamento, la comunicazione e la diffusione da parte dell'Università degli Studi del Piemonte Orientale "A. Avogadro" dei dati personali, trattati con o senza l'ausilio di mezzi elettronici, per il perseguimento dei propri fini istituzionali.
2. L'Università provvede al trattamento dei 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 e delle libertà fondamentali, nonché della dignità dell'interessato, con riferimento particolare alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Articolo 2 – Tipologie di dati trattati dall'Università

1. Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalle Leggi in materia di protezione dei dati personali e dal presente Regolamento.
2. L'Università degli Studi del Piemonte Orientale è un'istituzione pubblica di alta cultura che ha per finalità lo sviluppo del sapere critico e della sua trasmissione. L'Università opera per attuare il diritto allo studio con particolare riguardo ai capaci e meritevoli, anche di concerto con gli enti competenti in materia. Favorisce la qualità e l'efficacia dell'attività di formazione degli studenti e ne cura la preparazione professionale. Nel perseguimento dei suoi fini, assicura il rispetto della libertà di ricerca e della libertà di insegnamento costituzionalmente protetti. Individua, coordina e predispone i mezzi materiali e finanziari a ciò necessari, in rapporto alle esigenze ed alle risorse. L'Università garantisce il raggiungimento delle proprie finalità istituzionali per mezzo delle sue strutture didattiche e di ricerca, ed attraverso la conclusione di apposite convenzioni con istituzioni ed organismi di alta cultura nazionali ed esteri, operanti nel campo della didattica e della ricerca, e con enti pubblici e privati.
3. Per il perseguimento dei propri fini istituzionali, l'Università tratta generalmente tipologie di dati personali relativi a:

   a) personale dipendente, docente e tecnico amministrativo, in servizio, cessato e a contratto;

   b) persone fisiche partecipanti a concorsi banditi dall'Università;

   c) studenti iscritti a corsi di laurea, scuole di specializzazione, dottorati di ricerca, master di I e II livello, corsi di perfezionamento, o che hanno già terminato il proprio ciclo di studi;

   d) personale operante a vario titolo nell'Università quali borsisti, tirocinanti, visitatori e collaboratori con prestazione coordinata e continuativa, non rientrante nella categoria sub a);

e) soggetti non rientranti nelle categorie precedenti, che intrattengono rapporti con l'Università, trattati esclusivamente per fini amministrativi e contabili;
f) dati personali raccolti per fini di didattica e di ricerca.

4. Non rientrano tra le tipologie dei dati trattati dall'Università quelli delle strutture universitarie afferenti al Dipartimento di Scienze della Salute e al Dipartimento di Medicina Traslazionale e alla Scuola di Medicina convenzionate con il Servizio Sanitario Nazionale, rispetto alle quali il titolare deve essere identificato nell'Azienda Ospedaliera di accreditamento. 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 disposizioni impartite dal Titolare o dal Responsabile dell'Ente Ospedaliero.

Articolo 3 – Definizioni

1. Ai fini del presente Regolamento si applicano le definizioni elencate all'art. 4 del Decreto Legislativo 30 giugno 2003, n. 196. Si intende per:

Leggi in materia di protezione dei dati personali	Regolamento UE 2016/679 "GDPR" - D.Lgs 196/2003, come emendato dal D.Lgs 101/2018 "Codice in materia di protezione dei dati personali" - le linee guida e i provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali e le linee guida e i provvedimenti applicabili emessi dal Comitato Europeo per la protezione dei dati personali ("EDPB", ex Gruppo di lavoro Art. 29
Trattamento:	Qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.
Dati personali	Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Dati identificativi:	I dati personali che permettono l'identificazione diretta dell'interessato.
Dati appartenenti a categorie particolari (Art. 9 GDPR):	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Dato anonimo:	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
Titolare:	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile del trattamento:	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati personali per conto del titolare del trattamento.
Autorizzati:	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.
DPO	Responsabile della protezione dei dati ai sensi dell'articolo 37 del GDPR.
Interessato:	La persona fisica, cui si riferiscono i dati personali.
Comunicazione:	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Diffusione:	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Banca di dati:	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
Blocco:	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.
Misure di sicurezza:	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello di protezione richiesto in relazione ai rischi per le attività di trattamento di dati personali individuati dall'Università
Strumenti elettronici:	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
Autenticazione informatica:	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
Credenziali di autenticazione:	I dati ed i dispositivi in possesso di una persona da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione formale.
Parola chiave:	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Dati storici:	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato.
Scopi statistici:	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici.
Scopi scientifici:	Le finalità di studio ed indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Articolo 4 - Circolazione dei dati all'interno dell'Università

1. L'accesso e la comunicazione di dati personali tra le diverse strutture amministrative di servizio, didattiche e scientifiche dell'Università del Piemonte Orientale, sono generalmente limitate ai casi in cui ciò sia diretto al perseguimento dei fini istituzionali dell'ente. In questi

casi la diffusione delle informazioni è ispirata al principio della libera circolazione delle medesime.

2. Nei casi di cui al 1° comma, la richiesta di accesso o comunicazione dei dati avviene in via diretta e senza formalità. Essa, in ogni caso, deve essere adeguatamente motivata.
3. Qualora la richiesta di accesso o comunicazione dei dati sia giustificata da fini diversi e/o ulteriori rispetto a quelli indicati nel 1° comma, l'istanza deve essere presentata in forma scritta per permettere al responsabile del trattamento un esame specifico delle condizioni di legittimazione soggettiva e oggettiva del richiedente.
4. Ai fini dell'accesso ai dati sono equiparati alle strutture dell'Università gli organismi di controllo e di valutazione quali il Collegio dei Revisori, il Nucleo di Valutazione ed ogni altro organo a cui espresse disposizioni normative affidano tali compiti.

Articolo 5 - Circolazione dei dati all'esterno dell'Università

1. Al fine di favorire l'inserimento nel mondo del lavoro e della ricerca degli studenti che hanno conseguito il titolo conclusivo dei corsi di studi previsti nell'ambito dell' ordinamento didattico, l'Università può, su richiesta di soggetti pubblici o privati ovvero di propria iniziativa, comunicare e diffondere all'esterno i dati personali attinenti alla carriera degli studenti, alle loro competenze ed aspirazioni professionali, anche mediante inserimento dei dati in sito Internet o in altri circuiti informativi. In tali casi sarà compito dell'Università ottenere la preventiva autorizzazione degli studenti interessati (ai sensi dell'articolo 96 del Codice in materia di protezione dei dati personali), previa informativa ai sensi dell'art. 8 del presente regolamento.
2. Ogni richiesta proveniente da soggetti esterni e finalizzata ad ottenere la diffusione e la comunicazione dei dati personali detenuti dall'Università anche in banche dati deve essere scritta e motivata. Nella richiesta devono essere specificati gli estremi del richiedente, l'indicazione dei dati dei quali si chiede l'ostensione e lo scopo per il quale essi sono richiesti. L'Università, dopo aver valutato che la diffusione e la comunicazione dei dati siano compatibili con le proprie finalità istituzionali, sentito il parere del DPO designato, provvede alla trasmissione dei medesimi nella misura e secondo le modalità strettamente necessarie a soddisfare la richiesta.
3. La comunicazione o la diffusione di dati personali a soggetti privati o a enti pubblici economici è ammessa unicamente quando sia prevista da una specifica norma di legge o di regolamento che ne preveda la divulgazione.
4. La comunicazione e la diffusione dei dati personali detenuti dall'Università sono consentite quando:
   - siano previste da una norma di legge o regolamento;
   - siano necessarie per finalità di ricerca scientifica o di statistica;
   - siano richieste da forze di polizia, autorità giudiziaria, organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o sicurezza dello Stato o di prevenzione, accertamento o repressione di reati;
   - sia stata espressamente autorizzata dagli interessati.

PARTE II

I SOGGETTI CHE EFFETTUANO IL TRATTAMENTO E DIRITTI DELL'INTERESSATO

Articolo 6 – Responsabile della protezione dei dati personali (DPO) - Titolare - Responsabile – Autorizzato

1. L'Università degli Studi del Piemonte Orientale è titolare del trattamento dei dati personali, ivi compresi quelli contenuti nelle banche di dati relative alle strutture decentrate dell'Ateneo, nella persona del suo rappresentante legale, il Rettore pro-tempore.
   Al titolare competono le decisioni in ordine alle finalità ed alle modalità di trattamento di dati personali, ivi compresa la predisposizione di misure adeguate di sicurezza.
2. L'Università degli Studi del Piemonte Orientale ha proceduto alla designazione di un Responsabile della protezione dei dati personali (DPO), trovando piena applicazione quanto disposto dall'articolo 37 (1) (a) del GDPR. Il DPO assolve a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione delle Leggi in materia di protezione dei dati personali.
3. Il titolare del trattamento, coadiuvato dal DPO, organizza le attività di vigilanza e di controllo, verifica la rispondenza dei trattamenti effettuati alle modalità prescritte dal Regolamento.
4. Il titolare del trattamento, coadiuvato dal DPO, organizza le attività di formazione in relazione alla corretta applicazione delle Leggi in materia di protezione dei dati personali.
5. Nell'ambito dell'Università, articolata in strutture amministrative, di servizio, didattiche e scientifiche, il referente interno che si occupa delle tematiche relative al trattamento dei dati personali e delle banche dati è il responsabile della struttura all'interno della quale i dati personali o le banche dati sono gestiti per le finalità istituzionali della rispettiva unità organizzativa.
6. Nelle strutture amministrative il referente interno è il Dirigente di Divisione
7. Nelle strutture di servizio, didattiche e di ricerca, i referenti interni sono i Direttori di ogni singolo Dipartimento.
8. Il Titolare del trattamento dei dati, nella persona del Rettore pro-tempore, può comunque designare, con proprio provvedimento, uno o più referenti interni diversi dai soggetti sopra indicati.
9. I referenti interni, sotto il diretto controllo del Titolare, assicurano, anche tramite verifiche periodiche, che l'esercizio delle attività attinenti al trattamento e alla diffusione dei dati personali di terzi si svolga nel rispetto della normativa vigente e delle rispettive istruzioni impartite. Garantiscono, inoltre, l'attuazione delle misure di sicurezza dei dati.
10. L'Università può altresì individuare dei "Responsabili del trattamento" cui delegare il trattamento dei dati nell'ambito dell'esecuzione degli accordi intercorrenti tra l'Università e soggetti (enti e/o società) delegati ogni qualvolta tali Responsabili effettuino attività di trattamento per conto dell'Università.
11. Il Titolare del trattamento designa, con atto scritto, gli Autorizzati al trattamento dei dati operanti all'interno dell'Università. L'Autorizzato al trattamento è colui al quale viene assegnato dal Titolare, anche in via temporanea, il compito di svolgere le operazioni materiali inerenti al trattamento. Tale soggetto opera sotto il controllo del Titolare.

11. Gli Autorizzati devono trattare i dati personali attenendosi alle istruzioni ad essi impartite dal Titolare, sentito il parere dei responsabili delle strutture organizzative nel rispetto delle Leggi in materia di protezione dei dati personali.

Articolo 7 – Diritti dell'interessato

1. L'Interessato può esercitare i diritti previsti dagli articoli da 15 a 23 del GDPR.
2. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
3. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili del trattamento o autorizzati.
4. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
   d) la portabilità dei dati personali trattati dall'Università sulla base del consenso o per l'adempimento di disposizioni contrattuali;
5. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.
6. L'accesso ai dati personali è gratuito.
7. In caso di ulteriori copie dei dati personali richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi, secondo le tariffe indicate nel Tariffario relativo al rimborso dei costi di diritti di segreteria, ricerca e copia di documenti nell'ambito dei procedimenti di accesso documentale e civico generalizzato (allegato 1). Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Articolo 8 – Informativa

1. L'interessato, ai sensi degli articoli 13 e 14 del GDPR, deve essere debitamente informato ogni qualvolta si provveda alla raccolta dei dati personali circa:
   a) le finalità e le modalità del trattamento cui sono destinati i dati richiesti;
   b) la natura obbligatoria o facoltativa del conferimento dei dati richiesti;
   c) le conseguenze derivanti da un eventuale rifiuto a rispondere;
   d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
   e) i diritti di cui gode ai sensi degli articoli da 15 a 23 del GDPR;
   f) gli estremi identificativi del titolare e, se designato, del DPO.;
   g) i tempi di conservazione o i criteri utilizzati per determinarli dei dati personali;
   h) i trasferimenti di dati personali a paesi terzi siti fuori dallo Spazio economico europeo;
   i) l'esistenza di un processo decisionale automatizzato e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. L'informativa può essere resa oltre che individualmente, anche mediante forme di comunicazione di massa od annunci su pagine web.
3. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa sul trattamento dei dati personali.

PARTE III

REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

Articolo 9 - Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:
   - trattati in modo lecito e secondo correttezza e secondo i principi di cui all'articolo 5 del GDPR;
   - raccolti e registrati per scopi determinati, espliciti e legittimi, utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
   - esatti e, se necessario, aggiornati;
   - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
   - conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario per gli scopi per i quali i dati sono stati raccolti o successivamente trattati.
2. I sistemi informativi sono configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali e identificativi, in modo da evitarne il trattamento quando le finalità perseguite possano essere realizzate mediante il semplice uso di dati anonimi.

Articolo 10 - Valutazione di impatto sulla protezione dei dati personali (DPIA) e consultazione preventiva

1. Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Responsabile interno effettua, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali. Il DPO fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento ai sensi dell'art. 35 del Regolamento UE.
2. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.
3. La valutazione d'impatto sulla protezione dei dati è obbligatoria nei casi seguenti in cui il trattamento ha ad oggetto:
   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 su dette 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);
4. Il Responsabile interno o suo referente si consulta con il DPO anche per assumere la decisione di effettuare o meno la valutazione d'impatto. Tale consultazione e le conseguenti decisioni assunte dal Responsabile interno o suo referente devono essere documentate nell'ambito della valutazione d'impatto. Il Responsabile interno o suo referente è tenuto a documentare le motivazioni nel caso adotti condotte difformi da quelle raccomandate dal DPO.
5. Il Responsabile per la transizione digitale fornisce supporto al DPO per lo svolgimento della valutazione di impatto privacy.
6. L'Università, per il tramite del DPO, consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della valutazione di impatto (DPIA) condotta indicano l'esistenza di un rischio residuale elevato.
7. L'Università, per il tramite del DPO, consulta il Garante per la Protezione dei dati personali anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica. In particolare, la consultazione è obbligatoria ove non sia necessario il consenso per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

Articolo 11 - Trattamento per scopi storici, statistici o scientifici

1. Il trattamento di dati personali per finalità storiche, statistiche e di ricerca scientifica può sempre essere effettuato anche oltre il periodo di tempo previsto per gli scopi iniziali per i quali i dati sono stati raccolti o trattati.
2. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, l'Università comunica e diffonde a soggetti pubblici e privati, anche per via telematica, dati personali, con esclusione di quelli appartenenti a categorie particolari, relativi ad attività di studio e di ricerca di laureati, dottori di ricerca, ricercatori, docenti, esperti e tecnici.
3. In relazione al trattamento dei dati per gli scopi ivi delineati e in riferimento ad ogni aspetto non espressamente disciplinato si rinvia alle disposizioni delle Leggi in materia di protezione dei dati personali. In relazione al trattamento di dati storici sono salve le disposizioni di cui al D.Lgs. 281/1999. La consultazione di documenti conservati negli archivi storici dell'Università resta disciplinata dal D.Lgs. 490/1999, come modificato dal codice in materia di protezione dei dati personali.

Articolo 12 - Trattamento dei dati per la gestione del rapporto di lavoro

1. Ai fini del trattamento di dati personali per la gestione del rapporto di impiego si considerano di rilevante interesse pubblico le finalità di instaurazione e gestione del rapporto di lavoro (anche non retribuito e/o onorario) e di qualsiasi altra forma di impiego di risorse umane, anche non comportante la costituzione di un rapporto di lavoro subordinato. Si intendono ricompresi, in particolare, i trattamenti effettuati per le seguenti finalità:
   a) applicare la normativa in materia di pubblico impiego e assumere personale anche appartenente a categorie protette;
   b) garantire le pari opportunità;
   c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;
   d) adempiere agli obblighi connessi alla definizione dello stato giuridico ed economico relativamente al personale in servizio o in quiescenza;
   e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;
   f) applicare la normativa in materia di previdenza ed assistenza, anche con riferimento alla comunicazione di dati anche mediante reti di comunicazione elettronica, quella integrativa riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica;
   g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;
   h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;
   i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;

l) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi;

m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;

n) svolgere l'attività di indagine e ispezione presso soggetti pubblici;

o) valutare la qualità dei servizi resi e dei risultati conseguiti.

2. La diffusione dei dati di cui alle lettere m), n) ed o) del comma 1 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato.

Articolo 13 – Videosorveglianza

1. Nelle strutture dove sono in funzione degli strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio, deve essere affissa apposita informativa che informi il pubblico della presenza degli impianti e delle finalità perseguite attraverso la videosorveglianza. I pannelli devono essere affissi in prossimità degli ingressi alle strutture ed essere visibili da chi vi accede. È inoltre necessario rispettare i seguenti principi:

a. una limitazione delle modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell'immagine) avendo attenzione alla individuazione del livello di dettaglio della ripresa dei tratti somatici delle persone in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;

b. individuazione dei soggetti legittimati ad accedere alle registrazioni;

c. l'indicazione del soggetto e della struttura cui l'interessato può rivolgersi e dei diritti che può esercitare.

PARTE IV

LA SICUREZZA DEI DATI

Articolo 14 - Misure di sicurezza e analisi dei rischi

1. Ai sensi dell'art. 32 del GDPR, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

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.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica,

dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

PARTE V

RESPONSABILITÀ – ACCESSO AGLI ATTI

Articolo 15 – Ambiti di responsabilità

1. Il dipendente pubblico che richiede, riceve, tratta, o semplicemente ha notizia di dati è vincolato al rispetto del segreto d'ufficio di cui all'art. 15 del D.P.R. 10 Gennaio 1957 n. 3, così come sostituito dall'art. 28 della Legge 7 Agosto 1990 n. 241.
2. Le leggi in materia di protezione dei dati personali sanciscono che chiunque cagioni un danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento del danno ai sensi dell'articolo 2050 del codice civile.
3. Le responsabilità dei soggetti di cui all'art. 6 comprendono anche quella relativa alla mancata vigilanza sull'attività degli autorizzati al trattamento dei dati, all'omessa o inidonea informativa fornita all'interessato.
4. La responsabilità penale, espressamente prevista dagli artt. 167- 167-bis e ter-168del D.Lgs. 30 giugno 2003, n. 196, è personale. Essa è riferibile al titolare, al responsabile o all'autorizzato del trattamento, cui l'uso illegittimo o scorretto dei dati sia riferibile.

Articolo 16 – Diritto di accesso e tutela della riservatezza

1. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela, sono disciplinati dalla L. 241/1990.
2. L'esercizio del diritto d'accesso, qualora comporti la comunicazione di dati personali di terzi, deve essere limitato ai dati necessari a soddisfare il diritto stesso.
3. Resta fermo il principio per cui i conflitti tra diritto di accesso e riservatezza dei terzi devono essere risolti nel senso che l'accesso, finalizzato per la cura o la difesa di propri interessi legittimi, prevale rispetto all'esigenza di riservatezza, nei limiti però in cui esso è necessario alla difesa di un interesse giuridicamente rilevante.
4. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango pari ai diritti dell'interessato, ovvero è relativo a un diritto della personalità o altro diritto o libertà, fondamentali ed inviolabili.

PARTE VI

DISPOSIZIONI FINALI

Articolo 17 - Disposizioni finali

1. Per quanto non previsto nel presente Regolamento, si applicano le disposizioni delle Leggi in materia di protezione dei dati personali e le successive modificazioni ed integrazioni.
2. Sono esclusi dal presente Regolamento i trattamenti dei dati appartenenti a categorie particolari e relativi a condanne penali e reati che vengono disciplinati dall'apposito Regolamento.

Articolo 18 - Entrata in vigore

1. Il presente Regolamento entra in vigore il giorno dopo la sua emanazione, è pubblicato all'Albo dell'Ateneo ed è disponibile sul sito web dell'Università.