UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

REGOLAMENTO INTERNO PER LA PROTEZIONE DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO UE 2016/679 DEL PARLAMENTO E DEL CONSIGLIO EUROPEO RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI

Titolo	PROCEDURA DI GESTIONE DEI NUOVI TRATTAMENTI		
Data di emissione	22.12.2022	**Versione**	2.0

Sommario

PARTE 1 - DISPOSIZIONI GENERALI

ART. 1 - AMBITO DI APPLICAZIONE

Il presente regolamento disciplina il trattamento di dati personali effettuato dall'Università Campus Campus Bio-Medico di Roma (d'ora in poi solo "Università") in applicazione dei principi di cui al Regolamento UE 2016/679, di seguito riferito "Regolamento UE" a differenza del presente testo di seguito riferito "Regolamento interno".

Il presente Regolamento interno si applica a tutte le strutture organizzative dell'Università, didattiche e scientifiche, agli uffici amministrativi, di staff e di servizio.

Il presente Regolamento interno è articolato in tre parti: la PARTE 1 contiene le indicazioni generali riguardanti il Regolamento UE, i principi e le definizioni di base, la struttura organizzativa per la protezione dei dati personali che l'Università si è data; la PARTE 2 è destinata a tutte le strutture organizzative dell'Università che gestiscono le attività didattiche e i servizi amministrativi centrali; la PARTE 3 contenente la norma finale del presente Regolamento interno.
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 e della dignità dell'interessato, con riferimento alla riservatezza e al diritto alla protezione dei dati personali.

ART. 2 - DEFINIZIONI

Ai fini del presente Regolamento interno ed in conformità a quanto previsto dal Regolamento UE, si applicano le definizioni riportate all'Art. 4 del Regolamento UE stesso, qui riportate per estratto:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «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;

5) «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;

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

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «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;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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

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

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

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

   a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

   b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

   c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

   a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

   b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

ART. 3 - ASSETTO ORGANIZZATIVO PER LA PROTEZIONE DEI DATI PERSONALI

3.1 TITOLARE, REFERENTI INTERNI, DPO (DATA PROTECTION OFFICER) E "AUTORIZZATI A OPERARE SUI DATI".

L'Università è titolare dei dati personali detenuti, siano essi raccolti o meno in banche dati, automatizzate o cartacee.

I dati personali sono conservati a cura dei responsabili delle strutture organizzative a cui sono affidati i diversi trattamenti.

L'Università si è dotata di una struttura organizzativa per la protezione dei dati personali, che individua le seguenti figure organizzative:

- **Titolare**: l'Università Campus Bio-Medico di Roma in persona del legale rappresentante;
- **Referenti interni**: Responsabili pro-tempore degli uffici individuati per il coordinamento della protezione dei dati personali (**uffici delegati**);
- **Strutture istituzionali**: tutti gli Uffici, Aree, Dipartimenti che compongono l'organigramma formale dell'Università;
- **Persone autorizzate ad operare sui dati personali**: persone che hanno ricevuto una lettera di incarico che li autorizza – ai sensi degli artt. 29, 32 del Regolamento UE e 2- *quaterdecies* del d.lgs. 196/2003 ("Codice Privacy") – ad operare sui dati personali e fornisce loro le istruzioni per l'esecuzione dei compiti loro affidati in tale ambito;
- **DPO**: il DPO – Data Protection Officer – (o RPD – Responsabile Protezione Dati) opera in staff al Titolare per assicurare la conformità dei trattamenti alle disposizioni del Regolamento UE; costituisce punto di contatto per gli interessati e per l'Autorità nazionale (Garante privacy);
- **Area Sistemi informativi**: Il Responsabile dell'Area opera in staff al Titolare di concerto con il DPO al fine di assicurare la sicurezza informatica dei dati personali trattati.

Le suddette figure organizzative compongono il **Comitato per la protezione dei dati personali**.
Gli uffici delegati e i corrispondenti Referenti interni sono individuati sulla base del raggruppamento dei processi omogenei di trattamento dei dati personali (**Ambiti di trattamento**):

Ambito (Raggruppamento)	**Finalità**	**Ufficio delegato e Referente alla data di aggiornamento del presente Regolamento**
Servizi accademici (Università e didattica)	Gestione dell'intero ciclo della formazione; Processi nell'ambito didattico e scientifico: orientamento, selezione, immatricolazioni, laurea, post lauream, ecc.	Responsabile Area Servizi Accademici
Ambito del personale (Gestione dei trattamenti interni)	Attività gestionali prevalentemente interne, relative ai dipendenti, alla loro selezione, formazione, gestione economica, giuridica e previdenziale del	Direttore Risorse Umane

	personale, protezione e prevenzione sul luogo di lavoro, ecc.	
Ambito economico finanziario	Attività gestionali prevalentemente relative a soggetti esterni, contabilità, fatturazione attiva e passiva, recupero crediti, approvvigionamenti, ecc.	Direttore Area economico finanziaria
Ambito comunicazione (comunicazione istituzionale e brand management)	Gestione delle attività tese alla promozione delle attività universitarie e didattiche, comprese attività post-lauream professionalizzanti, reperimento fondi, adesione a iniziative ecc.	Responsabile Area Comunicazione istituzionale e brand management
Ambito attività operative	Gestione delle attività di videosorveglianza e controllo accessi	Direttore Operations

Il Servizio Legale e il suo Responsabile, ha particolare competenza per quanto riguarda:

- Cause civili e penali
- Contrattualistica

Qualora i dati siano gestiti su sistemi informatici amministrati dall'Area Sistemi Informativi, il Responsabile dell'Area è responsabile del trattamento dei dati limitatamente alle operazioni connesse con l'esercizio dei sistemi informatici contenenti i dati o le banche dati.

I soggetti designati quali **Referenti interni** in quanto **Responsabili pro-tempore degli uffici delegati**, sono nominati con provvedimento di "delega di funzione" del Titolare.

Il Titolare può designare, con proprio provvedimento, Responsabili esterni del trattamento dei dati personali ai sensi del Regolamento UE. Il Responsabile esterno effettua il trattamento attenendosi alle istruzioni impartite per iscritto dal Titolare.

I responsabili delle strutture istituzionali, che operano sotto il diretto controllo del Titolare, potranno rivolgersi, per ogni possibile dubbio o quesito riguardante dati personali, **all'ufficio delegato referente per uno specifico trattamento o al DPO**. I responsabili delle strutture istituzionali vigilano sull'osservanza del Regolamento interno e sul rispetto delle norme sulla privacy, riferendo al Referente dell'Ufficio Delegato preposto le problematiche, le non conformità, le azioni suggerite in materia di protezione dei dati personali.
I responsabili delle strutture istituzionali richiedono direttamente all'Area sistemi informativi l'attivazione dei profili autorizzativi per l'accesso ai sistemi informatici degli Autorizzati ad operare sui dati personali.

I profili autorizzativi attivati restano in carico all'Area Sistemi Informativi che ne conserva l'archivio storico.

3.2 CARATTERISTICHE E COMPITI DEL DPO (DATA PROTECTION OFFICER)

Il DPO (Data Protection Officer) o in italiano RPD (Responsabile della Protezione dei Dati) è una nuova figura introdotta dal Regolamento UE. Si ritiene utile pertanto riassumere le caratteristiche e i compiti di tale nuova figura.

Le principali caratteristiche del DPO sono sinteticamente di seguito riassunte:

- conoscenza delle normative e delle prassi nazionali ed europee in materia di protezione dei dati e del Regolamento;
- conoscenza dello specifico settore di attività e della struttura organizzativa del Titolare del trattamento, incluse le normative specifiche di settore nazionali e sovranazionali;
- buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal Titolare e intrinseche alle attività svolte;
- qualità personali comprendenti elevati standard deontologici atti ad assicurare l'osservanza delle disposizioni del Regolamento, l'aderenza ai principi fondamentali del trattamento, il rispetto dei diritti degli interessati;
- capacità relazionali atte ad assicurare una efficiente comunicazione con l'Autorità Garante nazionale, con gli interessati, con i colleghi ai fini della promozione della cultura della protezione dei dati all'interno dell'azienda;
- assenza di conflitto di interessi, in quanto il DPO può svolgere altre funzioni all'interno dell'azienda, ma non in posizioni nelle quali tali funzioni possano dare adito a conflitto di interessi relativamente alle decisioni in merito alle finalità e alle modalità dei trattamenti di dati personali;
- indipendenza ed obbligo di non ricevere istruzioni rispetto alla propria attività di DPO;
- il DPO non può essere rimosso o penalizzato per la propria attività come DPO.

L'Università ha stabilito nel dettaglio i compiti assegnati al DPO, che di seguito si riepilogano:

- informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento 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;

- fornire assistenza in merito alla valutazione d'impatto, per i diversi trattamenti (già esistenti prima della promulgazione del Regolamento UE, nuovi trattamenti e variazioni ai trattamenti esistenti), sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- gestire le richieste di esercizio dei diritti da parte degli interessati;
- gestire il Registro dei trattamenti.

Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
I riferimenti del DPO sono pubblicati sul sito internet dell'Università, all'interno delle informative privacy dell'Università e nella intranet istituzionale.

3.3 RAPPORTI CON LE STRUTTURE ISTITUZIONALI

L'organizzazione per la protezione dei dati personali ha il solo scopo di assicurare il controllo di conformità dei trattamenti di dati personali eseguiti dall'Università e il rispetto dei diritti, delle libertà e della dignità di tutti i soggetti interessati dai trattamenti eseguiti. Non ha quindi relazione con i rapporti gerarchici fra le strutture istituzionali, che sono intesi all'efficacia ed efficienza delle attività operative.
Le strutture istituzionali mantengono il loro compito di vigilare sul rispetto della riservatezza, integrità e disponibilità dei dati personali da loro trattati.
Con riferimento alla definizione dei profili delle persone autorizzate ad operare sui dati personali, ciascuna struttura aziendale provvede a comunicare all'Area Sistemi Informativi dell'Università le proprie esigenze di accesso ai dati. L'Area Sistemi Informativi provvede a inserire nei sistemi informatici le dovute autorizzazioni all'accesso previa i necessari controlli di autenticazione.
Gli archivi cartacei sono sotto la responsabilità delle strutture istituzionali a cui risultano assegnati dalla normativa oppure con riferimento all'attività da essi eseguita.

3.4 PROCEDURE

La protezione dei dati personali viene effettuata attraverso procedure che si applicano a specifiche trattamenti dei dati personali. Il personale dell'Università, i responsabili delle strutture istituzionali, i Referenti interni sono tenuti alla loro applicazione. Le situazioni dei trattamenti sono le seguenti:

- VIOLAZIONI DEI DATI PERSONALI
- RICHIESTE DI ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

- CONTROLLO E AGGIORNAMENTO DEL REGISTRO DEI TRATTAMENTI
- ISTITUZIONE DI NUOVI TRATTAMENTI
- VARIAZIONI A TRATTAMENTI ESISTENTI
- ESECUZIONE DEGLI AUDIT PERIODICI INTERNI
- ESECUZIONE DEGLI AUDIT RICHIESTI DA AUTORITA' DI CONTROLLO

L'Università provvede all'erogazione degli opportuni corsi di formazione volti all'illustrazione delle procedure e delle attività da compiersi da parte dei vari partecipanti al processo.
Le procedure sono pubblicate sulla intranet istituzionale dell'Università.

Con riferimento alla procedura relativa alle richieste di esercizio dei diritti degli interessati,
all'interessato spettano i diritti previsti dal Regolamento UE e precisamente:

- Diritto di accesso dell'interessato
- Diritto di rettifica
- Diritto alla cancellazione («diritto all'oblio»)
- Diritto di limitazione del trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione
- Diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che la riguardano o che incida in modo analogo significativamente sulla sua persona.

L'interessato può rivolgersi, per l'esercizio dei propri diritti, al Titolare, al DPO, a un Referente interno o a un responsabile di struttura aziendale, oppure segnalare attraverso un'apposita modulistica, disponibile nel sito web dell'Università, la volontà di esercitare il proprio diritto.
I diritti riferiti a dati personali di persone decedute possono essere esercitati da chi ha un interesse proprio ad agire o agisce a tutela della persona deceduta o per ragioni familiari meritevoli di protezione.

3.5 RACCOLTA DEI DATI, INFORMATIVA E CONSENSO

Ogni struttura aziendale dell'Università assolve agli obblighi di informativa nei confronti dell'interessato ogniqualvolta provvede alla raccolta dei dati personali, informando l'interessato sulla base dei formati di informativa predisposti e resi disponibili alle strutture istituzionali a seconda delle necessità relative a ciascun trattamento.
Le informative privacy in uso sono presenti nella Intranet istituzionale dell'Università.
L'informativa può essere resa oralmente (purché se ne possa dare prova), per iscritto presso le strutture o anche mediante informative di massa, come cartelli affissi nei locali in cui gli interessati si recano per conferire i dati o mediante annunci sulle pagine Web dell'Università.

Il personale a contatto con gli interessati raccoglie il consenso al trattamento, ove necessario per il perseguimento di specifiche finalità del trattamento previamente e dettagliatamente specificate all'interno dell'informativa privacy e nelle formule di consenso sottoposte agli interessati.
L'Università, mediante le proprie strutture, fornisce l'informativa rispetto ai dati raccolti presso l'interessato.

L'informativa privacy è fornita per iscritto e contiene:

1. in caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

   a) l'identità e i dati di contatto del titolare del trattamento;

   b) i dati di contatto del responsabile della protezione dei dati;

   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

   d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) (legittimo interesse del titolare), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

   e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

   f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

   a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

ART. 4 - REGOLE PER IL TRATTAMENTO DEI DATI

4.1 MODALITÀ DI RACCOLTA E REQUISITI DEI DATI PERSONALI

I dati personali oggetto di trattamento sono:

1. trattati in modo lecito e secondo correttezza;

2. raccolti e registrati per scopi determinati, espliciti e legittimi, utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
3. esatti e, se necessario, aggiornati;
4. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
5. 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.

I sistemi informativi sono configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali e identificativi, in modo da evitare il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o modalità di identificazione dell'interessato solo in caso di necessità.

L'Università tratta:

- dati personali diversi da quelli di cui all'art. 9 (categorie particolari di dati personali) e all'art. 10 (dati relativi a condanne penali e reati) del Regolamento UE;
- dati personali di cui all'art. 9 del Regolamento UE, con riferimento ai dati relativi all'appartenenza sindacale, alla salute (es. assenze per malattia), eventualmente all'origine razziale/etnica nell'ambito dei trattamenti del personale dipendente o assimilato ovvero nell'ambito dell'erogazione delle attività didattiche, con riguardo a esigenze speciali degli studenti (ad es. sussistenza di handicap, anche parziali);
- dati personali di cui all'art. 10 del Regolamento UE in relazione ad alcune specifiche attività di cura svolte dall'Università , solo qualora il trattamento avvenga sulla base del diritto dell'Unione o degli Stati membri;

4.2 TRATTAMENTO PER SCOPI STORICI, STATISTICI O SCIENTIFICI

Il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati e può essere effettuato anche oltre il periodo necessario a questi altri scopi.

Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico l'Università può utilizzare, comunicare e diffondere dati relativi ad attività di studio e di ricerca, dedotti dalle attività principali, a condizione che siano stati previamente anonimizzati in maniera tale che non sia possibile risalire all'identità dei soggetti (persone fisiche) a cui i dati si riferiscono.

Possono essere comunque diffusi dati personali resi pubblici dall'interessato rispettando il vincolo di destinazione degli stessi.

In relazione al trattamento di dati per scopi statistici o scientifici si rinvia alle disposizioni del Regolamento.

4.3 CESSAZIONE DEL TRATTAMENTO

In caso di cessazione del trattamento, per esaurimento delle finalità perseguite dal titolare, i dati sono, in alternativa:

1. distrutti,
2. restituiti ai soggetti ai quali si riferiscono prima della distruzione;
3. conservati per fini di difesa dei diritti in sede giudiziaria, per tutela interessi vitali, oppure con riferimento a disposizioni legislative e regolamentari; non sono oggetto di comunicazione per fini diversi da quelli elencati o diffusione;
4. conservati o ceduti ad altro titolare per scopi storici, statistici o scientifici in conformità alle disposizioni vigenti in materia, opportunamente anonimizzati e soggetti ad opportune misure di sicurezza.

ART. 5 - MISURE DI SICUREZZA

I dati personali oggetto di trattamento sono custoditi e controllati anche in ragione delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Per tutti i trattamenti, prima della loro messa in opera, viene valutato il livello di rischio ed effettuata, se il trattamento presenta rischi elevati per gli interessati, il DPIA (Data Protection Impact Assessment), individuando opportune misure organizzative e tecniche per la messa in sicurezza e la protezione dei dati. Qualora le misure aggiuntive dedotte dal DPIA non siano sufficienti a mitigare i rischi, il trattamento viene sottoposto a consultazione preventiva con l'Autorità di controllo (Garante per la protezione dei dati personali).

Per quanto riguarda la sicurezza dei trattamenti dei dati effettuati con l'ausilio di strumenti elettronici il titolare del trattamento opera secondo le modalità individuate nel Regolamento UE, nelle linee guida dell'Autorità di controllo e nella normativa di settore.

L'Università esegue con regolarità, anche con il supporto di società specializzate nell'ambito della cybersecurity, test di vulnerability assessment e di penetration test al fine di individuare tempestivamente falle di sicurezza e prevenire incidenti di sicurezza e violazioni dei dati personali.
L'utilizzo di piattaforme di software di base e d'ambiente allineate allo stato dell'arte dell'evoluzione tecnologica e un costante processo di aggiornamento garantiscono l'adeguata protezione dei dati contro codice malevolo, virus, malware.
L'Università ha in atto articolate procedure organizzative supportate da evoluti sistemi tecnici per il backup dei dati al fine di assicurare il recupero immediato di situazioni che possano implicare la perdita dei dati o l'integrità degli archivi.
L'Università si accerta, prima della messa in opera di piattaforme applicative complesse quali ad esempio il sistema informativo ospedaliero, che esse siano conformi alla legislazione nazionale e sovranazionale per quanto attiene il trattamento e la protezione dei dati personali.
L'Università provvede a nominare gli amministratori di sistema previsti dal provvedimento del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (come modificato in base al provvedimento del 25 giugno 2009) e provvede a mettere in opera il relativo sistema di "Log delle attività degli amministratori di sistema".
L'Università ha in atto una "Policy sugli strumenti IT" pubblicato nella intranet dell'Università, che riguarda l'utilizzo sia delle apparecchiature (computer) messe a disposizione dall'Università che quelle di proprietà di esterni, nonché per quanto riguarda la connessione in rete locale (anche wi-fi pubblico) e geografica e l'utilizzo della posta elettronica.

L'Università ha in atto un opportuno sistema di autenticazione e autorizzazione all'accesso per tutto quanto riguarda i dati personali, ed in particolare i dati sensibili, al fine di scongiurare accessi non autorizzati e conseguenti situazioni di trattamenti non consentiti (comunicazione o diffusione non autorizzata, alterazione, ecc.) da parte di soggetti non incaricati del trattamento (autorizzati al trattamento).

Ai Responsabili delle Strutture istituzionali a cui fanno capo i trattamenti e ai Referenti interni è richiesto di vigilare sul rispetto, da parte degli incaricati, delle misure di sicurezza.

Il trattamento di dati personali effettuato con strumenti elettronici è consentito previa adozione delle seguenti misure di sicurezza:

1. minimizzazione dei dati personali;
2. autenticazione informatica;
3. adozione di procedure di gestione delle credenziali di autenticazione;
4. utilizzazione di un sistema di autorizzazione;

5. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli apparecchi elettronici;
6. protezione degli strumenti elettronici e dei dati da trattamenti illeciti e accessi non consentiti;
7. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
8. adozione di tecniche di cifratura o di codici identificativi cifrati per determinati trattamenti (fra quelli che trattano "Categorie particolari di dati personali e dati relativi a condanne penali e reati"), fra i quali tecniche di pseudonimizzazione, criptazione e similari.

Il trattamento di dati senza l'ausilio di strumenti elettronici è consentito previa adozione delle seguenti misure:

1. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati al trattamento;
2. previsione di procedure per un'adeguata custodia di atti e documenti cartacei affidati agli incaricati per lo svolgimento dei relativi compiti;
3. previsione di procedure per la conservazione di determinati atti in archivi ad accesso protetto e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

I Referenti interni, il DPO e l'Area Sistemi Informativi garantiscono un servizio di supporto e di verifica per tutto ciò che riguarda la sicurezza dei trattamenti di dati e i connessi adempimenti previsti dal Regolamento UE e dal presente Regolamento interno.

ART. 6 - INIZIO, MUTAMENTO O CESSAZIONE DEL TRATTAMENTO DEI DATI

Per consentire al titolare di monitorare il trattamento dei dati personali, nonché di provvedere alle necessarie attività di valutazione del rischio e delle misure di sicurezza organizzative e tecniche necessarie per mitigare i rischi suddetti (privacy by design), nel caso di inizio, mutamento o cessazione di un trattamento che implichi il trattamento di dati personali, il responsabile di Area o il responsabile promotore del trattamento deve tempestivamente informare il **Referente interno** ed il **DPO**. L'informazione deve avvenire con congruo preavviso, in modo tale da consentire le necessarie analisi d'impatto. Nel caso di trattamenti che possano implicare alto rischio per i dati personali, l'informazione deve avvenire contestualmente all'inizio della fase di studio di fattibilità, anche per evitare al titolare costi che potrebbero risultare inutili a fronte di rischi così elevati da condurre ad un blocco della realizzazione del trattamento.

In caso di inizio di un nuovo trattamento la comunicazione contiene almeno:

a) le finalità e le modalità del trattamento;
b) la base giuridica su cui il trattamento si fonda
c) la natura dei dati personali, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono;
d) l'ambito di comunicazione e di diffusione dei dati;
e) gli eventuali trasferimenti di dati previsti verso Paesi non appartenenti all'Unione europea;
f) particolari categorie di dati soggetti a restrizioni sulla base del Regolamento UE o della normativa nazionale;
g) una descrizione delle misure di sicurezza adottate;
h) l'eventuale connessione con altri trattamenti o banche di dati;

e comunque ogni altra informazione utile al titolare per procedere alla valutazione del rischio e alle azioni conseguenti previste dal Regolamento.

Il Referente interno, ricevuta la comunicazione, convoca il gruppo di lavoro previsto dalle procedure:

- ISTITUZIONE DI NUOVI TRATTAMENTI
- VARIAZIONI A TRATTAMENTI ESISTENTI

di cui al precedente art. 3.4 e ne cura l'esecuzione. Le procedure citate sono sempre seguite dalla procedura di AGGIORNAMENTO DEL REGISTRO DEI TRATTAMENTI a cura del DPO.

ART. 7 - TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI (Art. 9 REGOLAMENTO UE) E DI DATI RELATIVI A CONDANNE PENALI O REATI (Art. 10 REGOLAMENTO UE)

Il trattamento dei dati di cui all'Art. 9 e all'Art. 10 del regolamento UE da parte dell'Università è consentito solo con riferimento al dettato del Regolamento UE, che integralmente si riporta:

1. è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il paragrafo 1 **non si applica** se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario 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, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dei principi di liceità del trattamento deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

È demandato al Referente interno nel cui ambito ricade il trattamento, verificare l'esistenza delle condizioni di cui sopra con l'assistenza del DPO.

I dati di cui al presente articolo sono raccolti presso l’interessato.

L’Università tratta dati di cui all’art. 9 e all’art. 10 del Regolamento UE solo qualora il trattamento sia necessario per lo svolgimento di attività istituzionali che non possono essere adempiute, caso per caso,

mediante il trattamento di dati anonimi o di dati personali di natura diversa. L'Università è autorizzata ad effettuare solo le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nel compimento di attività di vigilanza, di controllo o ispettive.

Per i dati di cui all'art. 9 e art. 10 del Regolamento UE contenuti in banche dati trattate con mezzi elettronici è necessario utilizzare tecniche di cifratura o codici identificativi o altre soluzioni che consentono di risalire all'interessato solo in caso di necessità.

L'Università predispone misure organizzative e strumenti operativi al fine di garantire la separazione dei dati idonei a rivelare lo stato di salute dagli altri dati personali, ove questi ultimi sono trattati per finalità che non richiedono l'utilizzo anche dei dati sanitari. Tali dati sono trattati con le modalità di cui al precedente comma anche quando sono tenuti in elenchi, registri, banche dati senza l'utilizzo di strumenti elettronici.

ART. 8 - TRATTAMENTO DEI DATI PER LA GESTIONE DEL RAPPORTO DI LAVORO

Si intendono riferiti all'ambito del rapporto di lavoro i trattamenti effettuati per le seguenti finalità:

a) gestione del personale appartenente alle categorie protette;
b) tutela delle pari opportunità;
c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi;
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;
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;
j) valutare la qualità dei servizi resi e dei risultati conseguiti.

ART. 9 - COMUNICAZIONE DEI DATI PERSONALI A ENTI ESTERNI ALL'UNIVERSITÀ

Le richieste rivolte all'Università e finalizzate ad ottenere il trattamento, la comunicazione o la diffusione di dati personali dovranno essere formulate per iscritto al Titolare, al Referente interno o al Responsabile della struttura aziendale coinvolta (il quale provvederà tempestivamente ad informare il Referente interno).

La comunicazione di dati personali a soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è necessaria per lo svolgimento di funzioni istituzionali dell'ente pubblico richiedente oppure quando il richiedente sia l'Autorità giudiziaria o di pubblica sicurezza.

La struttura aziendale che ha rapporti con l'ente richiedente deve tempestivamente rappresentare l'esigenza al titolare (o al Referente interno), al fine di pianificare l'intervento, raccogliere il gruppo di lavoro di cui al precedente Art. 7 ed avviare la procedura per l'istituzione del trattamento di comunicazione.

Le richieste provenienti da soggetti privati possono essere accolte soltanto se previste da norme di legge, regolamento, o da atti normativi speciali. Le richieste devono essere adeguatamente motivate e devono contenere:

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

La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dall'Autorità di controllo o dall'autorità giudiziaria:

- in riferimento a dati personali dei quali è stata ordinata la cancellazione ovvero quando è decorso il periodo di tempo per la loro conservazione;
- in riferimento a dati personali per i quali l'interessato abbia esercitato il diritto di cancellazione (oblio), di limitazione, di opposizione;

- per finalità diverse da quelle indicate nelle informative e per le quali si è ottenuto il consenso dell'interessato.

È fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati.

Nel rispetto dei limiti previsti dai commi precedenti e dei fini istituzionali dell'Università specificamente al fine di agevolare l'orientamento, la formazione e l'inserimento professionale degli studenti e dei laureati dell'Ateneo, è consentita la comunicazione di dati relativi a studenti e laureati dell'Università a soggetti pubblici e privati ed a consorzi interuniversitari che ne facciano richiesta in relazione alle predette finalità (incluso inviti ad incontri, manifestazioni, riunioni, congressi). I dati relativi agli esiti scolastici, intermedi e finali, individuati nell'informativa resa agli interessati, possono essere successivamente oggetto di trattamento esclusivamente per le finalità in base alle quali sono stati raccolti.

L'Università rilascia a terzi certificati contenenti dati personali relativi a studenti o laureati presso l'Ateneo, dietro esibizione di atto di delega sottoscritta dall'interessato, accompagnato da copia fotostatica di un documento d'identità del delegante e del delegato.

Le attività di contabilizzazione e fatturazione svolte dalle strutture istituzionali centrali (servizi centrali), sono effettuate sulla base fornita dall'assolvimento di un obbligo contrattuale, così come le successive attività di comunicazione agli enti pubblici preposti sono basati sul rispetto di una norma di legge.

Inoltre, i servizi centrali trattano dati personali nell'ambito della prevenzione e sicurezza del lavoro, sulla base della legislazione in vigore.

ART. 10 – ACCESSO AI DATI PERSONALI CHE COMPORTI LA COMUNICAZIONE DI DATI PERSONALI DI TERZI

L'esercizio del diritto d'accesso ex art. 15 del GDPR deve essere limitato ai dati relativi al solo interessato. In ogni caso, il diritto di ottenere l'accesso e una copia ai dati personali non deve ledere i diritti e le libertà altrui.

Quando il trattamento concerne dati idonei a rivelare lo stato di salute o all'appartenenza sindacale, 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.

ART. 11 - NOTIFICAZIONE E COMUNICAZIONE DI PARTICOLARI CATEGORIE DI TRATTAMENTO

La normativa nazionale di recepimento del Regolamento UE è stata consolidata con il d.lgs. 101/2018, che abroga l'art. 37 del d.lgs. 196/2003 concernente la notificazione al Garante di alcune particolari tipologie di trattamenti (dati genetici, biometrici, indicanti la posizione di persone o oggetti mediante rete di comunicazione elettronica, dati idonei a rivelare lo stato di salute e la vita sessuale, la sfera psichica, dati trattati con strumenti elettronici volti a definire il profilo e la personalità dell'interessato, dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi, per sondaggi, ricerche di mercato, dati relativi alla situazione di rischio di solvibilità economica, ecc.). Il presente articolo al momento quindi non si applica a causa dell'abrogazione del citato Art. 37, salvo successive determinazioni del Garante che saranno prontamente apportate in aggiornamento.

ART. 12 - VIDEOSORVEGLIANZA

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 dell'Università, 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.

Le caratteristiche, le modalità di funzionamento, accesso e conservazione delle immagini raccolte dai sistemi di videosorveglianza presenti nei locali dell'Università, nonché i relativi eventuali controlli da parte dell'Università, sono descritti all'interno della Policy sugli strumenti IT adottata dall'Università.

L'Università e la Fondazione Policlinico Universitario Campus Bio-Medico (di seguito "Fondazione") hanno stipulato una convenzione che ha lo scopo di creare una collaborazione rafforzata e sinergica tra le parti e che prevede, tra le altre cose, l'organizzazione e la condivisione di attrezzature e spazi in coworking che le parti hanno reciprocamente messo a disposizione per un uso congiunto.

L'Università e la Fondazione, al fine di dare esecuzione a quanto previsto nella convenzione suddetta hanno stipulato un accordo volto a regolamentare i reciproci obblighi e diritti in ordine all'utilizzazione degli spazi in coworking quali, specificatamente, il PRABB, il CESA e il laboratorio dell'Università, e delle relative attrezzature.
In virtù del predetto accordo e nei termini ivi previsti l'Università e la Fondazione, fra le altre cose, intendono installare e utilizzare un impianto di videosorveglianza all'interno degli spazi in coworking. L'utilizzo del sistema di videosorveglianza negli spazi in coworking risponde ad esigenze condivise quali, nello specifico, la tutela del patrimonio mobiliare e immobiliare e la sicurezza dei luoghi di lavoro, in quanto consente di prevenire eventi indesiderati – fra cui furti, rapine, danneggiamenti e, in generale, qualsiasi fatto illecito commesso ai danni di persone e/o cose - fungendo da deterrente e consentendo, a posteriori, la ricostruzione del contesto a seguito di una segnalazione di un evento indesiderato.

Rispetto al trattamento dei dati acquisiti per il tramite dell'impiego del predetto sistema di videosorveglianza negli spazi in coworking a tutti i fini connessi al rapporto di lavoro, compresi i fini disciplinari, l'Università e la Fondazione, quali soggetti che operano altresì in qualità di datori di lavoro, agiscono quali autonomi e distinti titolari del trattamento ciascuno rispetto al personale di propria competenza, nel rispetto delle garanzie previste dall'art. 4 della L. 300/1970 (di seguito "Statuto dei Lavoratori") e delle altre garanzie previste a tutela dei lavoratori. La visualizzazione, la trasmissione e l'utilizzo delle immagini raccolte tramite il sistema di videosorveglianza presente negli spazi in coworking per le predette finalità da parte dell'Università e/o della Fondazione in qualità di autonomi titolari, potrà avvenire solo ove sussistano esigenze fondate, ragionevoli e concrete connesse a finalità relative al rapporto di lavoro, nel rispetto delle garanzie previste dall'art. 4 dello Statuto dei Lavoratori e delle altre garanzie previste a tutela dei lavoratori.

Rispetto al trattamento dei dati personali derivante dall'installazione e dall'utilizzo del sistema di videosorveglianza negli spazi in coworking, l'Università e la Fondazione agiscono in qualità di contitolari del trattamento per il perseguimento delle seguenti finalità:

a) sicurezza delle persone e tutela del patrimonio mobiliare e immobiliare degli spazi in coworking, in particolare rispetto ed eventuali aggressioni, incidenti sul lavoro, furti, rapine, danneggiamenti e atti di vandalismo, nonché per esigenze organizzative e produttive;
b) trasmissione delle immagini raccolte tramite i sistemi di videosorveglianza installati presso gli spazi in coworking all'Università e/o alla Fondazione, autonomi titolari del trattamento, per tutti i fini connessi al rapporto di lavoro, compresi i fini disciplinari, ove sussistano esigenze fondate, ragionevoli e concrete

connesse a finalità relative al rapporto di lavoro, nel rispetto delle garanzie previste dall'art. 4 dello Statuto dei Lavoratori e delle altre garanzie previste a tutela dei lavoratori;
c) accertamento, esercizio e/o difesa di un diritto in sede giudiziaria, in ambito stragiudiziale nonché nelle fasi che precedono il contenzioso;
d) adempimento di ogni eventuale obbligo normativo incombente sulle parti, ivi inclusi gli ordini emanati dalle autorità giudiziarie e di polizia.

L'attività descritta comporta il trattamento di dati personali appartenenti alla categoria dei dati comuni consistenti, essenzialmente, nelle immagini raccolte dal sistema di videosorveglianza che ritraggono gli interessati, potenzialmente anche in volto, nonché, con riferimento alle attività di accesso alle immagini di videosorveglianza, informazioni connesse ai log di accesso alle immagini registrate.

Sul punto si rinvia:
i) all'accordo di contitolarità stipulato tra la Fondazione e l'Università che disciplina (ex art. 26 del GDPR), le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR. Tale accordo riflette i rispettivi ruoli e i rapporti dei contitolari con gli interessati e il suo contenuto essenziale è messo a disposizione degli interessati che ne facciano richiesta;
ii) alla *Procedura Videosorveglianza aree coworking (PRABB, CESA, laboratorio Policlinico)*.

ART. 13 – AMBITO DELLA RESPONSABILITÀ

Chi richiede i dati, chi li riceve, chi li tratta è comunque vincolato al rispetto del dovere di riservatezza ed è tenuto ad adottare tutte le misure necessarie a garantire la sicurezza dei dati a lui trasmessi.

La responsabilità, anche penale, prevista dalla normativa sovranazionale (Regolamento UE) e nazionale per un eventuale uso dei dati personali conosciuti non conforme alle indicazioni impartite dal titolare, resta a carico della singola persona cui l'uso illegittimo sia imputabile.

La responsabilità del dipendente dell'Università per **colpa o negligenza lieve** viene sanzionata sulla base del contratto di lavoro e del Regolamento del personale.
La responsabilità per **colpa o negligenza grave** che abbia comportato danni finanziari o di immagine all' Università o a terzi interessati, oltre alla sanzione suddetta potrà essere ulteriormente soggetta a rivalsa economica da parte dell'Università stessa.
La responsabilità per **dolo** è perseguita sulla base della legislazione vigente dalle autorità competenti, e comporta sanzioni penali, rivalsa economica da parte dell'Università, provvedimenti previsti dal contratto di lavoro e dal Regolamento del personale.

PARTE 2 – UNIVERSITA’

ART. 14 – TIPOLOGIE DEI DATI TRATTATI DALL'UNIVERSITÀ

L'Università assicura la qualità e l'efficacia della propria attività di formazione culturale degli studenti e ne cura la preparazione professionale, assumendo le opportune iniziative al fine di orientare e favorire l'inserimento nel mondo del lavoro dei propri studenti. L'Università persegue le proprie finalità attraverso le sue strutture didattiche, e mercé la conclusione di accordi con istituzioni ed organismi italiani, stranieri, comunitari ed internazionali, operanti nel campo della didattica e della ricerca e con enti pubblici e privati.

Per il perseguimento dei propri fini istituzionali l'Università tratta principalmente le seguenti tipologie di dati personali:

1. dati relativi al personale dipendente e a contratto, docente e non docente;
2. dati relativi a studenti, ivi compresi coloro che hanno già terminato gli studi e categorie assimilate;
3. altro personale operante a vario titolo nell'Università quali borsisti, tirocinanti, visitatori, etc.;
4. dati raccolti per fini amministrativi e contabili;
5. dati raccolti per fini di didattica e di ricerca.

Questi dati possono appartenere anche alla categoria di dati particolari ex art. 9 del Regolamento UE (es. soggetti appartenenti a categorie protette; portatori di handicap; etc.).

ART. 15 – PRESENZA DI STUDENTI NEI PERCORSI DI CURA PER ATTIVITA' FORMATIVE

Lo svolgimento delle attività formative professionalizzanti rivolte a studenti tirocinanti e specializzandi richiede, in occasione dell'erogazione delle prestazioni sanitarie da parte del professionista sanitario presso il Policlinico a favore dei pazienti, la partecipazione e il coinvolgimento degli studenti iscritti ai corsi di laurea e post-laurea presso l'Università. Con specifico riguardo alla presenza degli studenti tirocinanti, si precisa che, al fine di limitare il disagio e in relazione al grado d'invasività del trattamento, verrà circoscritto il numero degli stessi presenti in occasione della prestazione sanitaria erogata in favore del paziente e si garantirà il rispetto di sue eventuali legittime volontà contrarie, senza che venga compromesso l'accesso alla prestazione sanitaria richiesta.

ART. 16 – MINIMIZZAZIONE DEI DATI PERSONALI

Nell'ambito delle procedure concorsuali, procedure selettive, procedure relative alla carriera universitaria degli studenti, laurea, corsi di specializzazione, procedure amministrative riguardanti la contribuzione etc., sono richiesti, raccolti e conservati i soli dati personali necessari per il raggiungimento delle finalità dei trattamenti.

ART. 17 – STRUMENTAZIONE INFORMATICA

Docenti e studenti dell'Ateneo possono utilizzare:

- strumentazione informatica messa a disposizione dall'Ateneo;
- strumentazione informatica propria (computer portatile) previa autorizzazione dell'Area Sistemi informativi;

la strumentazione informatica messa a disposizione del personale dell'Università dovrà essere utilizzata in conformità delle norme riportate nel documento **"Policy sugli strumenti IT"** pubblicato nella intranet dell'Università, sia per quanto riguarda l'utilizzo delle apparecchiature che per quanto riguarda la connessione in rete locale e geografica e l'utilizzo della posta elettronica.

ART. 18 – INFORMATIVE

Gli schemi di informativa per orientamento, immatricolazione, laurea, post lauream sono riportati nella intranet dell'Università.
Sono ivi riportate anche le informative riguardanti il personale dipendente e il corpo docente.
Le informative in uso sono presenti nella Intranet dell'Università.
L'informativa può essere resa oralmente (purché se ne possa dare prova), per iscritto presso le strutture, o anche mediante informative di massa, come cartelli affissi nei locali in cui gli interessati si recano per conferire i dati o mediante annunci sulle pagine Web.
Il personale a contatto con gli interessati, oltre a fornire l'apposita informativa privacy, raccoglie il consenso dell'interessato, ove necessario per il perseguimento di specifiche finalità del trattamento previamente e dettagliatamente specificate all'interno dell'informativa privacy e nelle formule di consenso sottoposte agli interessati.

ART. 19 – L'UNIVERSITA' QUALE RESPONSABILE DEL TRATTAMENTO

L'Università può stipulare contratti e convenzioni con soggetti esterni, nei quali si prevede l'assegnazione di compiti specifici all'Università che potrebbero comportare il trattamento dei dati personali da parte dell'Università per conto di tali soggetti esterni, configurandosi un rapporto nel quale l'Università risulta Responsabile del trattamento ai sensi del Regolamento UE. In tal caso l'Università deve essere formalmente designata "Responsabile del trattamento" da parte del Titolare, l'Università provvederà a definire un Responsabile interno, coincidente con un Referente interno (ufficio delegato) che, in collaborazione con il DPO dovrà definire le misure organizzative e tecniche atte a garantire la conformità con il Regolamento UE, sulla base delle specifiche istruzioni del titolare del trattamento.

ART. 20 – TRASFERIMENTO DI DATI ALL'ESTERO PER ATTIVITA' DI COOPERAZIONE SCIENTIFICA, DI FORMAZIONE, DI JOB PLACEMENT, RICERCA FINANZIATA, ECC.

Nell'ambito delle attività internazionali e di supporto agli studenti, nel loro particolare interesse, l'Università può trasferire i dati personali verso enti terzi localizzati in paesi extra UE.
In tal caso l'Università si impegna affinché detti trasferimenti avvengano in presenza di condizioni legittimanti il trattamento previste agli artt. 47 e ss. del Regolamento UE e vengano adottate misure tecniche idonee per effettuare tali trasferimenti sulla base delle raccomandazioni previste nell'annex 2 del "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*", adottate dall' *European Data Protection Board (*EDPB) il 10 Novembre 2020.

ART. 21 – ATTIVITÀ NELL'AMBITO DELLA RICERCA SCIENTIFICA

Inoltre, l'Università e la Fondazione Policlinico Universitario Campus Bio-Medico hanno stipulato una Convenzione che ha lo scopo, tra le altre cose, di creare una collaborazione rafforzata e sinergica tra le Parti per lo svolgimento delle attività di ricerca scientifica, al fine di creare una sovrastruttura funzionale ("Piattaforma") alle predette attività attraverso l'organizzazione di risorse umane (ad esempio studenti, tirocinanti, docenti, ricercatori, medici ecc.), attrezzature e spazi che le Parti hanno reciprocamente messo a disposizione per un uso congiunto, nel rispetto delle rispettive autonomie e competenze. Le Parti sono dunque contitolari dei trattamenti effettuati per la gestione congiunta della predetta Piattaforma, costituita dall'organizzazione di uomini e mezzi messi a disposizione da ciascuna parte, funzionalmente legata all'esecuzione di tutti i trattamenti finalizzati alla realizzazione delle predette attività. Al riguardo si rinvia all'Accordo di contitolarità stipulato tra la Fondazione e l'Università che disciplina (ex art. 26 del GDPR), le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR. Tale accordo riflette i rispettivi ruoli e i rapporti dei contitolari con gli interessati e il suo contenuto essenziale è messo a disposizione degli interessati che ne facciano richiesta.

Art. 22 - ATTIVITA' DI RACCOLTA FONDI

L'Università e la Fondazione Policlinico Universitario Campus Bio-Medico hanno stipulato una convenzione che ha lo scopo di creare una collaborazione rafforzata, sinergica e integrata tra le Parti per lo svolgimento delle attività assistenziali, didattiche, di ricerca scientifica e di terza missione. Tra le altre cose, attraverso la predetta convenzione, l'Università e la Fondazione si sono obbligate ad assicurare il coordinamento e l'integrazione delle iniziative e delle attività di fundraising principalmente nei settori della formazione universitaria, della ricerca bio-medica e ingegneristica, dell'assistenza ospedaliera e ambulatoriale, in termini di strategie, attività e modalità. Rispetto al trattamento dei dati

personali di persone fisiche svolto nell'ambito delle attività di fundraising, quindi l'Università e la Fondazione sono contitolari dei trattamenti effettuati.

L'attività di fundraising comporta il trattamento di informazioni appartenenti alla categoria dei dati comuni di tipo anagrafico (nome, cognome, data di nascita, codice fiscale), professionale e fiscale (partita IVA), di contatto (indirizzo, numero di telefono, l'indirizzo e-mail), di pagamento (numero carta di credito), nonché informazioni relative alla donazione effettuata, per le seguenti finalità:
(i)per gestione amministrativo-contabile della donazione**,** sulla base dell'art. 6.1.b) del GDPR**;**
(ii) per le finalità promozionali e di informazione sulle attività nei settori della formazione universitaria, della ricerca bio-medica e ingegneristica, dell'assistenza ospedaliera e ambulatoriale condotte dai contitolari, comprese l'attività di *costumer satisfaction* e *l'invio di newsletter*, al fine di promuovere campagne di raccolta fondi a favore degli stessi, attraverso strumenti automatizzati (sms, mms, e-mail, sistemi di chiamata automatizzati senza operatore, utilizzo dei social network, whatsapp) e non (posta ordinaria, telefono con operatore), sulla base dell'art. 6.1.a) del GDPR;
(iii) solo nei confronti dei contatti regolari (tali possono essere anche le donazioni regolari), per attività che rientrano tra gli scopi istituzionali individuati nell'atto costitutivo o nello statuto dei Contitolari, come l'invio di messaggi di promozione di raccolte fondi nei settori della formazione universitaria, della ricerca bio-medica e ingegneristica, dell'assistenza ospedaliera e ambulatoriale, attraverso strumenti non automatizzati (quali posta cartacea e telefono con operatore), sulla base dell'art. 6.1.f) del GDPR;
(iv) per inviare messaggi di promozione di raccolte fondi personalizzate, sulla base dell'art. 6.1.a) del GDPR;
(v) per adempiere ad eventuali obblighi previsti dalla legge, o soddisfare richieste provenienti dalle autorità, sulla base dell'art. 6.1.c) del GDPR;
(vi) per finalità difensive che si rendano necessarie per i contitolari sulla base degli artt. 6.1.f) e 9.2.f) del GDPR;
(vii) anonimizzazione dei dati per valutazioni di tipo statistico e di mercato, sulla base degli artt. 5, par. 1, lett. b) e 6, par. 4 e Considerando 50 del Regolamento. Al riguardo si rinvia all'Accordo di contitolarità stipulato tra la Fondazione e l'Università che disciplina (ex art. 26 del GDPR), le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR. Tale accordo riflette i rispettivi ruoli e i rapporti dei contitolari con gli interessati e il suo contenuto essenziale è messo a disposizione degli interessati che ne facciano richiesta.

Art. 23 - ATTIVITA' DIDATTICHE E DI FORMAZIONE PRE E POST-LAUREA PROFESSIONALIZZANTE

Attraverso la convenzione predetta, l'Università e la Fondazione hanno creato una collaborazione rafforzata e sinergica anche per lo svolgimento delle attività didattica e di formazione pre e post laurea professionalizzante. Nel trattamento dei dati personali per lo svolgimento delle predette attività, l'Università e la Fondazione agiscono in qualità di contitolari del trattamento; in particolare, il trattamento dei dati personali svolto in contitolarità attiene principalmente alla finalità di gestione e rendicontazione delle attività didattiche e formative svolte dai tirocinanti e specializzandi. Al riguardo si rinvia all'Accordo di contitolarità stipulato tra la Fondazione e l'Università che disciplina (ex art. 26 del GDPR) le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR. Tale accordo riflette i rispettivi ruoli e i rapporti dei contitolari con gli interessati e il suo contenuto essenziale è messo a disposizione degli interessati che ne facciano richiesta.

PARTE 3 - NORMA FINALE

Per quanto non previsto nel presente Regolamento interno si applicano le disposizioni normative del Regolamento UE, del Codice Privacy e dei provvedimenti dell'Autorità Garante per la protezione dei dati personali applicabili in materia.

Il presente Regolamento interno sarà sottoposto a revisione periodica dalla data della sua emissione.