UNIVERSITÀ
CAMPUS BIO-MEDICO DI ROMA

"MODELLO ORGANIZZATIVO PRIVACY"

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

ART. 1 – INTRODUZIONE E AMBITO DI APPLICAZIONE

Il presente Regolamento Interno per la protezione dei dati personali (di seguito anche solo "il Documento" o "Regolamento Interno"), adottato dall'Università Campus Bio-Medico di Roma (di seguito anche solo "Università" o "Ateneo"), costituisce il documento interno mediante il quale l'Ateneo disciplina in modo organico e sistematico i principi, le responsabilità e le modalità operative concernenti il trattamento dei dati personali nell'ambito delle proprie attività istituzionali, didattiche, scientifiche e amministrative.

La redazione del documento si fonda sui precetti del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito "Regolamento" o "GDPR") e del decreto legislativo 30 giugno 2003, n. 196(c.d. "Codice Privacy), come modificato dal decreto legislativo 10 agosto 2018, n. 101, nonché sui provvedimenti e sulle linee guida emanate dal Garante per la Protezione dei Dati Personali e dall'*European Data Protection Board*.

Più in particolare, il presente documento individua le strategie, le linee guida generali e le disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dall'Università. Al suo interno sono definiti i ruoli, le responsabilità e gli adempimenti da seguire in materia di protezione dei dati personali, e deve ritenersi applicabile a tutte le strutture organizzative dell'Ateneo: didattiche, scientifiche, amministrative, di staff e di servizio.

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

«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;

«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;

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

«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;

«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;

«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;

«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;

«Data Protection Officer» ("DPO") o «Responsabile della protezione dei dati»: soggetto, interno o esterno all'organizzazione aziendale, nominato obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal titolare del trattamento o dal responsabile del trattamento. Il DPO deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assistere il Titolare o il Responsabile nel garantire il rispetto della normativa in materia di protezione dei dati personali. Svolge, in condizioni di autonomia e indipendenza, attività di consulenza, sorveglianza e controllo sull'osservanza del GDPR e delle policy interne. Funge da punto di contatto per l'Autorità di controllo e per gli interessati, fornisce pareri (anche in merito alle DPIA), promuove la corretta individuazione di responsabili e autorizzati al trattamento, cura la formazione e la sensibilizzazione del personale e vigila complessivamente sull'adeguatezza dei trattamenti svolti dall'organizzazione.

«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;

«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;

«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;

«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;

«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;

«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;

«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;

«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;

«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;

«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;

«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;

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

«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;

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

«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;

«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;

«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;

«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;

«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 – RIFERIMENTI NORMATIVI

Il presente documento è redatto in conformità al quadro normativo e regolatorio vigente in materia di protezione dei dati personali e sicurezza delle informazioni, con particolare riferimento alle seguenti fonti:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 ("Regolamento");
- D.lgs. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali" o "Codice Privacy"), come modificato dal D.lgs. 10 agosto 2018, n. 101;
- Provvedimenti, linee guida e raccomandazioni dell'Autorità Garante per la protezione dei dati personali, ove applicabili;
- Linee guida, raccomandazioni e best practice emanate dall'European Data Protection Board (EDPB) e, ove pertinenti, dal Gruppo di lavoro ex art. 29 (WP29);
- Legge 20 maggio 1970, n. 300 ("Statuto dei Lavoratori"), con particolare riferimento all'art. 4

(controlli a distanza), ove applicabile;

- Normativa nazionale e unionale di settore applicabile alle attività istituzionali dell'Università, con particolare riguardo ai trattamenti connessi a didattica, gestione del personale, amministrazione/contabilità, comunicazione istituzionale e attività di ricerca;

Le presenti fonti devono intendersi richiamate anche in riferimento alle successive modifiche e integrazioni, nonché agli orientamenti interpretativi e applicativi delle Autorità competenti e della giurisprudenza rilevante.

ART. 4 - ASSETTO ORGANIZZATIVO PER LA PROTEZIONE DEI DATI PERSONALI

4.1 Figure coinvolte nel trattamento dei dati personali

L'Università è Titolare dei dati personali trattati e detenuti per il perseguimento delle proprie finalità istituzionali, come definite dallo Statuto e dai regolamenti di Ateneo, indipendentemente dal fatto che tali dati siano raccolti in banche dati informatizzate o in archivi cartacei. I dati personali sono conservati all'interno dei sistemi di archiviazione adottati dall'Ateneo, nel rispetto delle misure organizzative e di sicurezza previste dal modello di governance privacy. La gestione e la custodia dei dati avvengono sotto la responsabilità delle direzioni e degli uffici competenti per i relativi trattamenti.

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

– **Titolare del trattamento**: l'Università Campus Bio-Medico di Roma, nella persona del suo Presidente.

– **Incaricati/Autorizzati al trattamento**: soggetti (quali, ad esempio, personale docente, personale amministrativo, ricercatori, collaboratori, stagisti, ecc.) che, in ragione della funzione o della mansione svolta, operano sui dati personali di titolarità di Università e, a tal fine, hanno ricevuto dal Titolare del trattamento un'autorizzazione scritta – ai sensi degli artt. 29, 32 del Regolamento e 2- quaterdecies del d.lgs. 196/2003 ("Codice Privacy") – al trattamento dei dati personali, contenente le istruzioni operative per l'esecuzione dei compiti loro affidati in tale ambito;

– **Chief Information Security Officer (CISO)**: Responsabile della sicurezza informatica dell'Università, incaricata di definire, implementare e supervisionare la strategia di sicurezza

informatica dell'Ateneo. Sovraintende alla protezione delle infrastrutture digitali, elabora le politiche e gli standard di sicurezza, coordina la gestione degli incidenti informatici e assicura la valutazione continua dei rischi, in conformità alle procedure e ai regolamenti interni adottati dall'Ateneo. Supporta il Titolare del trattamento nella definizione delle misure di sicurezza dei dati personali e collabora con il DPO e con il Responsabile della Direzione Sistemi Informativi per garantire la corretta applicazione delle misure tecniche e organizzative di sicurezza a tutela dei dati personali e dei sistemi informativi.

– **Data Protection Officer ("DPO"):** Il Responsabile della Protezione dei Dati dell'Università, figura interna all'Ateneo, svolge attività di consulenza, sorveglianza e controllo sull'osservanza del GDPR in relazione ai trattamenti di dati personali effettuati dall'Università. Agisce come punto di contatto per l'Autorità di controllo e per gli interessati, fornisce pareri - anche in materia di DPIA - e supporto interpretativo sulla normativa privacy, promuove la corretta individuazione di responsabili e soggetti autorizzati al trattamento, cura la formazione e la sensibilizzazione del personale e vigila complessivamente sull'adeguatezza dei trattamenti. Collabora inoltre in stretto raccordo con il Titolare, il CISO e il Responsabile della Direzione Sistemi Informativi per assicurare la piena conformità dei trattamenti alle disposizioni del Regolamento;

– **Direzione Sistemi informativi**: Nella figura del Responsabile della Direzione Sistemi Informativi, responsabile della gestione e della sicurezza delle infrastrutture informatiche e dei sistemi informativi dell'Università. Nell'ambito della protezione dei dati personali, cura l'attuazione e il mantenimento delle misure tecniche e organizzative di sicurezza, in conformità alle procedure e ai regolamenti applicabili adottati dall'Ateneo. Opera in stretto raccordo con il DPO e il CISO per garantire l'efficace protezione e sicurezza dei dati personali trattati dall'Ateneo;

– **Amministratori di sistema interni**: personale designato tale, dedicato alla gestione di uno o più "impianti di elaborazione con cui vengano effettuati trattamenti di dati personali compresi i sistemi di gestione delle basi di dati" e che pertanto accedono in modo privilegiato a risorse del sistema informativo;

– **Amministratori di sistema esterni**: persone giuridiche o fisiche designate tali nell'ambito di un Accordo sul trattamento dati e nomina di Responsabile del trattamento ex art. 28 del Regolamento che si occupano della gestione e/o manutenzione di server, siti web, software anche complessi con cui vengano effettuati trattamenti di dati personali e a cui spetta il compito

di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio.

– **Referente/i Interno/i**: i responsabili pro-tempore di Direzione, Area, Servizio, Ufficio o Unità Operativa che, nell'ambito delle rispettive competenze, possono essere coinvolti dai soggetti sopra menzionati per il coordinamento delle attività e delle questioni inerenti alla protezione dei dati personali, con riferimento ai trattamenti ricadenti nelle aree di propria responsabilità.

I Referenti Interni sono individuati sulla base del raggruppamento dei processi omogenei di trattamento dei dati personali (Ambiti di trattamento):

Direzione, Area, Servizio, Ufficio o Unità Operativa	**Ambito di trattamento**	**Referente Interno alla data di aggiornamento del presente Regolamento**
Servizi accademici	Gestione dell'intero ciclo della formazione; Processi nell'ambito didattico e scientifico: orientamento, selezione, immatricolazioni, laurea, ecc.	**Responsabile Area Servizi Accademici**
Ambito del personale	Attività gestionali prevalentemente interne, relative ai dipendenti, alla loro selezione, formazione, gestione economica, giuridica e previdenziale del personale, protezione e prevenzione sul luogo di lavoro, ecc.	**Direttore Risorse Umane**
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 e Fundraising**
Ambito attività operative	Gestione delle attività di videosorveglianza e controllo accessi	**Direttore Operations**

Attività di ricerca scientifica	Ricerca scientifica e sperimentazioni cliniche in ambito medico-biomedico ed epidemiologico	**Responsabile Area Ricerca**
Formazione Post-Lauream	Attività di formazione post lauream (master, corsi di perfezionamento, corsi executive)	**Responsabile UCBM Academy**

I Referenti interni, che operano sotto il diretto controllo del Titolare, potranno rivolgersi al DPO per ogni possibile dubbio o quesito riguardante il trattamento dei dati personali. I Referenti interni forniscono il loro supporto al DPO sull'osservanza del Regolamento interno e sul rispetto della normativa in materia di protezione dei dati personali, assicurando la tempestiva segnalazione al DPO di eventuali criticità, non conformità o interventi correttivi ritenuti opportuni nell'ambito delle aree di rispettiva competenza.

4.2 Caratteristiche e compiti del DPO (Data Protection Officer)

L'Università ha designato un Responsabile della Protezione dei Dati (Data Protection Officer - DPO) ai sensi degli artt. 37 e ss. del Regolamento (UE) 2016/679. I compiti del DPO sono definiti dall'art. 39 del Regolamento e dettagliati nel presente Modello organizzativo, nel rispetto dei requisiti di indipendenza e delle garanzie previste dall'art. 38 del Regolamento.
Il Titolare riconosce nel DPO il presidio tecnico-giuridico principale del proprio sistema di protezione dei dati personali, attribuendo a tale figura il compito di fungere da raccordo tra le esigenze operative dell'Università e gli obblighi derivanti dal diritto europeo e nazionale.

In particolare, il DPO:

- fornisce informazioni e consulenza al Titolare del trattamento e al personale che partecipa alle operazioni di trattamento in merito agli obblighi derivanti dal Regolamento e dalle altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati personali;
- sorveglia l'osservanza del Regolamento, delle altre disposizioni applicabili e delle politiche interne del Titolare in materia di protezione dei dati personali, anche con riferimento all'attribuzione di responsabilità, alla sensibilizzazione e alla formazione del personale coinvolto e alle connesse attività di controllo;
- fornisce parere in merito allo svolgimento della valutazione d'impatto sulla protezione

dei dati (DPIA) e ne sorveglia l'esecuzione ai sensi dell'art. 35 del Regolamento;

- coopera con l'Autorità di controllo e funge da punto di contatto per quest'ultima per questioni connesse al trattamento, inclusa, se del caso, la consultazione preventiva;
- supporta la gestione delle richieste di esercizio dei diritti da parte degli interessati, secondo le procedure interne adottate dall'Università;
- supporta la tenuta e l'aggiornamento del Registro delle attività di trattamento, nonché il complessivo presidio documentale della conformità.

Con specifico riferimento al compito di sorvegliare l'osservanza della normativa (art. 39, par. 1, lett. b), GDPR), l'attività del DPO si sostanzia in un controllo sulla conformità dei trattamenti alla disciplina vigente e al sistema documentale interno, mediante: (i) la raccolta di informazioni utili a identificare e descrivere le attività di trattamento; (ii) l'analisi e la verifica di conformità dei trattamenti, incluse le misure tecniche e organizzative adottate; (iii) attività di informazione, consulenza e raccomandazioni indirizzate al Titolare e alle strutture competenti, anche in un'ottica di miglioramento continuo del modello di gestione privacy in termini di adeguatezza, efficienza ed efficacia.

Il DPO svolge la funzione di sorveglianza sia su richiesta del Titolare (in particolare nei casi in cui è opportuna o dovuta la consultazione preventiva), sia di propria iniziativa, sulla base di valutazioni autonome e del rischio. In via esemplificativa, il DPO valuta l'opportunità di interventi di verifica e approfondimento ogniqualvolta vengano avviati nuovi trattamenti o modificate in modo significativo attività di trattamento esistenti, intervengano cambiamenti rilevanti nel quadro normativo/organizzativo, emergano segnalazioni di potenziali non conformità, ovvero si verifichino violazioni dei dati personali o incidenti di sicurezza (anche presunti).

Il DPO è chiamato a svolgere attività di sorveglianza di carattere sistematico su base periodica, indipendentemente da segnalazioni di non conformità, cambiamenti nel quadro normativo e/o nei trattamenti, al fine di cogliere eventuali variazioni che potrebbero passare inosservate. Tale attività viene svolta, in particolare:

- attraverso la programmazione di visite di audit a campione, con i Responsabili delle funzioni/strutture rilevanti dal punto di vista privacy di volta in volta individuate;
- attraverso richieste di informazioni e documentazione indirizzate ai Responsabili delle funzioni/strutture rilevanti dal punto di vista privacy di volta in volta individuate;
- attraverso la programmazione di un'attività di verifica di più ampio spettro, volta a

ripercorrere il complesso delle attività di trattamento svolte dall'Università per realizzare una mappatura aggiornata delle stesse, con eventuale formalizzazione in un documento di ricognizione e analisi degli scostamenti (gap analysis) e delle azioni di miglioramento.

Le attività di controllo di cui sopra vengono programmate per tempo dal DPO e comunicate al Presidente del Consiglio di Amministrazione dell'Università, secondo le prassi interne.

Il DPO è chiamato a valutare la conformità alla normativa in materia di protezione dei dati personali anche a seguito di richiesta di parere da parte del Titolare e/o di attività di verifica richiesta dallo stesso. La consultazione preventiva del DPO da parte del Titolare è da considerarsi obbligatoria, in particolare, nei seguenti casi:

a) in tutti i casi in cui debbano essere assunte decisioni che impattano sul trattamento dei dati personali (ad es. sviluppo interno o esterno di prodotti/sistemi basati su nuove tecnologie), affinché il DPO possa valutarne la conformità normativa, le analisi dei rischi operate dal Titolare, nonché le misure di protezione dei dati e di sicurezza adottate by design e by default;

b) in caso di valutazione d'impatto sulla protezione dei dati (DPIA o Data Protection Impact Assessment) ex art. 35 del Regolamento;

c) in caso di Violazione dei Dati Personali (data breach) o altro incidente, secondo quanto previsto dalla procedura per la gestione dei data breach;

d) in caso di esercizio dei diritti da parte degli interessati, secondo quanto previsto dalla procedura per la gestione dei diritti degli interessati.

Nel caso in cui la sorveglianza richiesta al DPO riguardi una DPIA, una violazione dei dati personali o altro incidente di sicurezza (anche presunto), ovvero l'esercizio dei diritti da parte degli interessati, si rinvia a quanto definito nelle relative procedure interne.

Le attività di sorveglianza possono essere svolte in loco e/o da remoto, anche mediante acquisizione ed esame della documentazione ritenuta rilevante (anche a campione), richieste di informazioni alle strutture competenti, organizzazione di incontri/interviste e, ove opportuno, somministrazione di questionari. Le strutture, i Referenti interni e il personale coinvolti nei trattamenti sono tenuti a collaborare mettendo a disposizione le informazioni richieste, nel rispetto dei principi di correttezza, riservatezza e minimizzazione.

Il DPO riferisce direttamente e funzionalmente al Presidente del Consiglio di Amministrazione del Titolare. A tal fine, oltre a comunicazioni episodiche volte a informare

tempestivamente il Presidente del Consiglio di Amministrazione di eventi rilevanti per i quali potrebbe rendersi necessaria un'azione correttiva e/o migliorativa, il DPO predispone una Relazione annuale sull'attività svolta. La Relazione annuale rendiconta, in modo organico, le attività eseguite in attuazione dei compiti previsti ex lege ai sensi dell'art. 39 del GDPR e del presente Modello, evidenziando eventuali non conformità, rischi e opportunità di miglioramento, nonché le misure raccomandate, le priorità e le tempistiche suggerite. Resta fermo che la determinazione finale e l'adozione delle decisioni organizzative e gestionali competono al Titolare del trattamento.

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 istituzionale dell'Università, nelle informative privacy e nella intranet istituzionale.

4.3 Responsabili del Trattamento

Ogni qualvolta un soggetto terzo (fornitore, consulente, service provider) svolga servizi per conto dell'Università che comportino il trattamento di dati personali per conto del Titolare (ad es. servizi payroll, piattaforme applicative e gestionali, hosting e cloud, manutenzione e assistenza IT, provider di posta elettronica, piattaforme di marketing, servizi di ricerca svolti in outsourcing, ecc.), tale soggetto è qualificato come Responsabile del trattamento ai sensi dell'art. 28 del Regolamento e deve essere formalmente designato prima dell'avvio delle attività di trattamento.

La designazione del Responsabile del trattamento avviene mediante contratto o altro atto giuridico, anche in forma elettronica, che vincoli il Responsabile al Titolare e che disciplini il trattamento svolto per conto dell'Università. Tale atto deve definire, almeno, durata, natura e finalità del trattamento, tipologia di dati personali, categorie di interessati, nonché obblighi e diritti del Titolare, includendo le clausole minime inderogabili previste dall'art. 28, par. 3, GDPR. Il Responsabile tratta i dati personali esclusivamente su istruzione documentata del Titolare, nel rispetto delle misure tecniche e organizzative concordate e degli ulteriori vincoli previsti nell'accordo di nomina.

Nel modello organizzativo privacy dell'Università, i Referenti interni competenti per l'attivazione/gestione del rapporto contrattuale con il fornitore, previa valutazione e supporto del DPO, provvedono: (i) alla valutazione di adeguatezza del fornitore sotto il profilo della

protezione dei dati personali (inclusa, ove applicabile, la verifica delle misure di sicurezza e delle garanzie offerte); (ii) alla verifica e predisposizione dello schema di nomina a Responsabile del trattamento conforme all'art. 28 GDPR; (iii) alla designazione formale dei fornitori che trattano dati personali per conto dell'Università, mediante sottoscrizione dell'apposito accordo di nomina ex art. 28 GDPR, assicurando che tale accordo sia perfezionato prima dell'inizio delle attività di trattamento.

Fermo restando quanto previsto nell'accordo di nomina, i principali obblighi del Responsabile del trattamento includono, in particolare:

- garantire che le persone autorizzate al trattamento alle proprie dipendenze siano vincolate da obblighi di riservatezza e che siano applicate misure idonee a proteggerne confidenzialità e integrità;
- adottare misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR, anche in ottica di protezione dei dati by design e by default, e assicurare la resilienza dei sistemi e la capacità di ripristino in caso di incidente;
- non ricorrere ad altri responsabili (sub-responsabili) senza la previa autorizzazione scritta del Titolare (specifica o generale) e, in ogni caso, garantire che eventuali sub-responsabili assumano obblighi sostanzialmente equivalenti a quelli previsti nell'accordo principale;
- assistere il Titolare nel dare seguito alle richieste di esercizio dei diritti degli interessati e nel rispetto degli obblighi in materia di DPIA, consultazione preventiva e gestione di violazioni dei dati personali, secondo quanto previsto dalle procedure interne dell'Università;
- mettere a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR e consentire e cooperare alle attività di verifica, incluse ispezioni e audit, svolte dal Titolare o da soggetti da questo incaricati;
- al termine della prestazione dei servizi, restituire e/o cancellare i dati personali trattati per conto dell'Università, salvo obblighi di conservazione previsti dalla normativa applicabile, secondo le istruzioni del Titolare e quanto disciplinato nell'accordo.

La corretta qualificazione dei fornitori, la formalizzazione della nomina ex art. 28 GDPR e il monitoraggio degli obblighi del Responsabile costituiscono elementi essenziali del presente Modello organizzativo, in quanto presidiano il rischio connesso all'esternalizzazione di attività di trattamento e garantiscono il mantenimento del controllo del Titolare sulle istruzioni e sugli

standard di sicurezza e conformità applicabili.

4.4 L'Università quale responsabile del trattamento

L'Università può stipulare contratti o convenzioni con soggetti esterni che prevedano l'assegnazione di compiti specifici la cui esecuzione comporti il trattamento di dati personali per conto dei medesimi soggetti. In tali ipotesi, l'Ateneo assume il ruolo di Responsabile del trattamento e deve, ai sensi dell'art. 28 del Regolamento, essere formalmente designata come tale dal Titolare, attraverso un contratto o un altro atto giuridico. L'Università provvederà a individuare il Referente interno che, in collaborazione con il DPO, sarà tenuto a garantire la conformità del trattamento svolto in qualità di Responsabile del trattamento al Regolamento e alle specifiche istruzioni impartite dal Titolare.

L'Università tiene traccia delle attività eseguite in qualità di Responsabile del trattamento attraverso un apposito Registro dei trattamenti, in ossequio a quanto disposto dall'art. 30 par. 2 del Regolamento.

4.5 Incaricati/Autorizzati al Trattamento

L'Università, in qualità di Titolare del trattamento e, ove applicabile, di Responsabile del trattamento, assicura che le persone autorizzate al trattamento dei dati personali ai sensi dell'art. 29 del Regolamento e dell'art. 2-quaterdecies del Codice Privacy operino sulla base di istruzioni documentate e nel rispetto di specifici obblighi di riservatezza.

All'atto dell'instaurazione del rapporto di lavoro o di collaborazione, ciascuna persona autorizzata riceve e sottoscrive la lettera di autorizzazione al trattamento, contenente le istruzioni operative riferite ai trattamenti svolti nell'ambito delle funzioni assegnate e l'impegno alla riservatezza, che permane anche successivamente alla cessazione del rapporto. Unitamente alla lettera di autorizzazione, l'Università mette a disposizione la procedura sull'uso e l'assegnazione delle risorse informatiche, richiamata per *relationem* nella documentazione di nomina e consultabile in ogni momento sulla intranet istituzionale, contenente indicazioni in merito alla gestione delle credenziali, all'utilizzo della posta elettronica, della rete e degli strumenti messi a disposizione dall'Università. La persona autorizzata riceve inoltre i riferimenti alle procedure interne rilevanti, tra cui la procedura di

gestione delle violazioni dei dati personali (data breach).

I Referenti interni richiedono direttamente alla Direzione Sistemi Informativi l'attivazione dei profili autorizzativi per l'accesso ai sistemi informatici degli Autorizzati ad operare sui dati personali/Autorizzati al trattamento. I profili autorizzativi attivati sono di competenza della Direzione Sistemi Informativi, che si avvale per le richieste e la conservazione delle istanze della piattaforma https://ucbm.freshservice.com/

Per specifiche funzioni che presentano un livello di rischio più elevato (es. Amministratori di Sistema), l'Università prevede istruzioni ulteriori e più stringenti, formalizzate in apposite designazioni e regole operative, coerenti con la normativa applicabile e con le misure di sicurezza adottate.

A completamento del presidio documentale, l'Università, con il supporto del DPO, promuove con periodicità almeno annuale attività di formazione e sensibilizzazione in materia di protezione dei dati personali, finalizzate a rafforzare la consapevolezza del personale e a garantire l'aggiornamento rispetto a procedure interne, misure di sicurezza e principali novità normative e indirizzi delle Autorità competenti.

Attraverso l'insieme di istruzioni documentate, procedure interne e formazione, l'Università attua misure organizzative idonee a garantire un trattamento dei dati personali conforme ai principi del Regolamento e orientato alla tutela dei diritti e delle libertà degli interessati.

4.6 Amministratori di sistema

Gli Amministratori di Sistema sono individuati e gestiti in coerenza con il 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" del 27 novembre 2008, pubblicato in G.U. n. 300 del 24 dicembre 2008 ("Provvedimento").

Alla luce di tale riferimento, sono considerati Amministratori di Sistema le figure tecniche - interne o, se del caso, in outsourcing (con identificazione delle persone fisiche incaricate) - che, in via stabile e non meramente occasionale, svolgono attività di gestione e manutenzione di sistemi informatici che trattano dati personali e che, per ruolo e privilegi, possono incidere su autenticazione e autorizzazioni, profili e privilegi di accesso, configurazioni di sistema, basi di dati/reti/apparati di sicurezza, nonché su backup e ripristino. Le funzioni sono attribuite tramite

designazione individuale con definizione degli ambiti di operatività consentiti; l'elenco è mantenuto aggiornato dalla Direzione Sistemi Informativi in apposito documento interno e l'operato degli Amministratori di Sistema è sottoposto a verifica almeno annuale, al fine di assicurarne la conformità alle mansioni attribuite e alle misure organizzative, tecniche e di sicurezza adottate dall'Università.

4.7 Procedure e Policy interne in materia di protezione dei dati personali

Al fine di assicurare una gestione strutturata e uniforme degli adempimenti in materia di protezione dei dati personali, **il Titolare del trattamento ha definito e adottato specifiche procedure interne**, volte a regolamentare i processi interni che comportano il trattamento di dati personali.

Tali procedure, formalizzate attraverso apposite *policy* applicabili ai singoli trattamenti, costituiscono parte integrante del sistema organizzativo dell'Università e sono vincolanti per i Referenti interni e tutto il personale dell'Università, ognuno in relazione alle proprie funzioni e competenze. I destinatari sono pertanto tenuti a conoscerle, rispettarle e assicurarne la corretta applicazione nello svolgimento delle proprie funzioni.

Le procedure sono pubblicate sulla intranet istituzionale dell'Università e sono le seguenti:

- Policy per il trattamento dei dati nell'area di ricerca e relativo allegato *Modulo nuovo progetto di ricerca*
- Procedura di gestione delle violazioni dei dati personali;
- Procedura di valutazione di impatto sulla protezione dei dati;
- Procedura di gestione dei diritti dell'interessato;
- Privacy Policy sul trasferimento di dati personali fuori dallo Spazio Economico Europeo (SEE);
- Procedura di gestione degli audit interni;
- Procedura di gestione degli audit di un'Autorità di controllo;
- Policy per la gestione di nuovi trattamenti, con relativo *Modulo nuovo evento*
- Policy di gestione variazione dei trattamenti;
- Policy di gestione del registro dei trattamenti;

Le procedure adottate sono rese disponibili sulla intranet istituzionale dell'Università, garantendone l'accessibilità a tutto il personale. Ogni membro del personale e i Referenti interni sono informati delle procedure vigenti attraverso i canali di comunicazione interni nonché tramite rinvio per relationem riportato all'interno delle lettere di nomina a persona autorizzata di cui agli artt. 29 del Regolamento e 2-quaterdecies del Codice Privacy. L'elenco seguente riporta le principali policy attualmente in vigore, con la precisazione che potrà essere aggiornato periodicamente per includere nuove procedure o modifiche a quelle esistenti. L'aggiornamento delle procedure è curato dal DPO, il quale assicura che contenuti e prescrizioni delle procedure e delle policy siano oggetto di periodica verifica e revisione, anche in funzione di modifiche organizzative interne e dell'evoluzione del quadro normativo, regolatorio e giurisprudenziale in materia di protezione dei dati personali, nonché degli indirizzi e provvedimenti delle Autorità competenti.

L'Università, con il supporto del DPO, 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.

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 esercitare i propri diritti rivolgendosi al DPO dell'Università all'indirizzo **dpo@unicampus.it,** riportato in tutte le informative rese dal Titolare e nelle *privacy policy* pubblicate sui siti web istituzionali dell'Ateneo.

4.8 Raccolta dei dati, informativa e consenso

L'Università, in qualità di Titolare del trattamento, assolve agli obblighi di informazione nei confronti degli interessati, di cui all'art. 12 del Regolamento, ogniqualvolta procede alla raccolta dei dati personali degli stessi, fornendo loro le informazioni relative al trattamento mediante le informative predisposte dal Titolare, con il supporto del DPO, e rese disponibili ai Referenti Interni di Direzione, Area, Servizio, Ufficio o Unità Operativa, che procederanno a fornirle agli interessati nell'ambito dei trattamenti di rispettiva competenze. Le informative sul trattamento dei dati personali sono rilasciate, per iscritto, ai sensi dell'art. 13 del Regolamento quando i dati personali sono raccolti direttamente presso gli interessati, e ai sensi dell'art. 14, quando le informazioni non sono ottenute direttamente da questi ultimi.

L'informativa privacy è resa agli interessati in forma scritta, mediante consegna di documentazione cartacea presso le strutture competenti per lo specifico trattamento e/o tramite strumenti di informazione "di massa" (ad es. cartellonistica, avvisi e QR Code affissi nei locali in cui l'interessato si reca per conferire i dati e/o dove avviene la raccolta del dato personale). Ove applicabile, l'informativa è altresì resa disponibile attraverso i canali digitali e web dell'Università, assicurandone la facile reperibilità e consultazione.

Il personale che intrattiene rapporti con gli interessati garantisce la messa a disposizione dell'informativa riferita allo specifico trattamento e, ove il consenso costituisca la base giuridica, provvede a raccoglierlo secondo le modalità previste, in relazione a finalità determinate, esplicite e puntualmente descritte nell'informativa e nelle relative formule di consenso.

In ogni caso, l'Università, per il tramite delle proprie strutture competenti, assicura che l'informativa sia fornita con riferimento ai dati personali raccolti direttamente presso l'interessato, prima o al più tardi al momento della raccolta.

L'informativa privacy contiene:

- l'identità e i dati di contatto del Titolare del trattamento e del DPO;
- le finalità e le basi giuridiche del trattamento, incluse le eventuali situazioni di legittimo interesse perseguite dal Titolare o da terzi;
- le categorie di destinatari cui i dati personali possono essere comunicati e, se del caso, l'intenzione di trasferire i dati verso un Paese terzo o un'organizzazione internazionale, unitamente alle garanzie adeguate previste dagli articoli 44 e seguenti del Regolamento;
- il periodo di conservazione dei dati personali o, se non determinabile, i criteri utilizzati

per stabilirlo;

– l'indicazione dei diritti riconosciuti agli interessati (accesso, rettifica, cancellazione, limitazione, opposizione e portabilità dei dati), nonché del diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali;

- la specificazione dell'eventuale obbligo legale o contrattuale di conferire i dati personali e delle conseguenze del mancato conferimento;
- l'esistenza di processi decisionali automatizzati, compresa la profilazione, e la logica, l'importanza e le conseguenze previste di tali trattamenti.

Quando i dati non sono raccolti presso l'interessato, l'informativa rilasciata ai sensi dell'articolo 14 del Regolamento riporta, in aggiunta a quanto sopra indicato, le categorie dei dati personali trattati e la fonte da cui essi provengono, specificando, ove applicabile, se si tratti di fonti accessibili al pubblico.

In tali casi, l'informativa è fornita all'interessato entro un termine ragionevole, comunque non superiore a un mese dal momento della raccolta dei dati, o, se i dati sono utilizzati per comunicare con l'interessato, al più tardi al momento della prima comunicazione, ovvero prima della loro comunicazione a terzi.

L'Università si è dotata di un *Registro delle informative privacy* in formato excel al fine di tenere traccia di tutte le informative in uso presso le varie strutture organizzative (servizi accademici, academy, risorse umane, comunicazione e fundraising etc..).

ART. 5 – PRINCIPI PER IL TRATTAMENTO DEI DATI

Il trattamento dei dati personali effettuato dall'Università Campus Bio-Medico di Roma si conforma ai principi generali stabiliti dal Regolamento.

Il Titolare del trattamento assicura che tutti i trattamenti di dati personali siano eseguiti nel rispetto dei principi di liceità, correttezza e trasparenza, di limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione, di cui all'articolo 5 del Regolamento.

5.1 Liceità, correttezza e trasparenza

Ogni trattamento è fondato su un'idonea base giuridica tra quelle previste dall'articolo 6 del Regolamento e, ove necessario, sul consenso libero, specifico e informato dell'interessato.

Le informazioni relative ai trattamenti sono rese agli interessati in forma chiara, completa e facilmente accessibile, secondo quanto disposto dagli articoli 12 e seguenti del Regolamento, con indicazione delle finalità, delle basi giuridiche, dei diritti esercitabili e delle modalità di contatto del DPO.

5.2 Limitazione delle finalità e minimizzazione dei dati

I dati personali sono raccolti e trattati esclusivamente per finalità determinate, esplicite e legittime, in relazione alle funzioni istituzionali dell'Università, ai progetti di ricerca, alle attività didattiche nonché agli adempimenti amministrativi, contabili e contrattuali correlati.
La raccolta dei dati è limitata a quelli strettamente pertinenti e necessari rispetto agli scopi per i quali vengono trattati; ogni trattamento eccedente o non proporzionato rispetto alle finalità dichiarate è da ritenersi inammissibile.

5.3 Esattezza e aggiornamento dei dati

Il Titolare del trattamento adotta procedure idonee a garantire che i dati personali siano esatti, completi e costantemente aggiornati. Le strutture istituzionali provvedono periodicamente alla verifica della correttezza delle informazioni contenute nei propri archivi e sistemi informativi, anche mediante il coinvolgimento diretto degli interessati (studenti, corpo docenti, etc.), ai quali è riconosciuto il diritto di rettifica dei dati che li riguardano.

5.4 Limitazione della conservazione

I dati personali sono conservati per un arco temporale non superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti e trattati.
Il Titolare definisce criteri di conservazione differenziati in funzione delle tipologie di trattamento, delle finalità perseguite e delle categorie di dati trattati, assicurando che, decorso il periodo di conservazione, i dati siano cancellati, anonimizzati o archiviati in forma non identificabile.

5.5 Integrità e riservatezza

Le misure di sicurezza tecniche e organizzative sono adottate in base a un approccio fondato sulla valutazione del rischio, tenendo conto della natura dei dati trattati, della complessità dei

sistemi informativi e delle potenziali minacce, al fine di prevenire trattamenti non autorizzati o illeciti e di scongiurare la perdita, la distruzione o il danneggiamento, anche accidentali, dei dati personali.

5.6 Responsabilizzazione

L'attività dell'Università, in qualità di Titolare del trattamento, è incentrata sul principio di responsabilizzazione (c.d. *accountability*), inteso quale dovere sostanziale di garantire, per quanto attiene alle decisioni e ai processi interni che riguardano il trattamento dei dati personali, la piena dimostrabilità della conformità al Regolamento.

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

Al fine di consentire al Titolare del trattamento di monitorare in modo efficace le operazioni sui dati personali e di valutare i rischi connessi, nonché le misure tecniche e organizzative idonee a mitigarli, ogni Referente Interno è tenuto a informare tempestivamente il DPO di ogni nuovo trattamento, della modifica di trattamenti esistenti o della loro cessazione.

L'informazione deve avvenire con congruo preavviso, in modo tale da consentire le necessarie analisi e l'eventuale valutazione del rischio. Nel caso di trattamenti di dati personali che possano comportare un rischio elevato per i diritti e le libertà delle persone fisiche, la comunicazione al Titolare deve intervenire contestualmente all'avvio della fase di studio di fattibilità, al fine di consentire la tempestiva valutazione della liceità e della sostenibilità del trattamento e di prevenire l'impiego di risorse in progetti che, per l'entità del rischio, potrebbero non risultare attuabili.

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

a) le finalità e le modalità del trattamento;
b) la natura dei dati personali, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono;
c) l'ambito di comunicazione e di diffusione dei dati;
d) gli eventuali trasferimenti di dati previsti verso Paesi o organizzazioni nazionali al di fuori dello Spazio Economico Europeo (SEE);
e) particolari categorie di dati soggetti a restrizioni sulla base del Regolamento o della normativa nazionale;
f) una descrizione delle misure di sicurezza adottate;

g) l'eventuale connessione con altri trattamenti o banche di dati;

e comunque ogni altra informazione utile al Titolare e al DPO per procedere alla valutazione del rischio e alle azioni conseguenti previste dal Regolamento. A supporto, il Referente interno e/o il soggetto promotore del trattamento può utilizzare il modulo allegato alla "Procedura di gestione dei nuovi trattamenti".

Invece, in caso di cessazione del trattamento, per esaurimento delle finalità perseguite dal Titolare, i dati personali sono, in alternativa:

- distrutti in modo sicuro e definitivo, mediante procedure e misure tecniche e organizzative idonee a impedirne il recupero, la ricostruzione o la re-identificazione, o resi anonimi in maniera irreversibile
- restituiti all'interessato, ove richiesto e ove applicabile, prima della distruzione;
- conservati limitatamente a ulteriori finalità lecite che ne giustifichino la permanenza in capo al Titolare, quali, a titolo esemplificativo, finalità difensive connesse all'esercizio o alla difesa di un diritto in sede giudiziaria, esigenze di compliance e dimostrazione dell'adempimento di obblighi normativi; in tali casi, i dati sono sottoposti a limitazione d'uso e di accesso, nonché a misure di minimizzazione, e non possono essere comunicati o diffusi per finalità ulteriori incompatibili.

ART. 7 – TIPOLOGIE DEI DATI TRATTATI DALL'UNIVESITÀ

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, riconducibili alle aree di trattamento sotto elencate.

1) Servizi accademici

(Gestione dell'intero ciclo della formazione; processi didattici e scientifici: orientamento, selezione, immatricolazioni, laurea, post lauream, ecc.)

A titolo esemplificativo, l'Università tratta: dati anagrafici e identificativi; dati di contatto; dati relativi a orientamento e selezione; dati di immatricolazione/iscrizione; dati di carriera

accademica (piano di studi, frequenze ove previste, esami, votazioni, tesi, conseguimento titolo, certificazioni); dati relativi a tirocini e stage; dati amministrativo-contabili connessi alla carriera (tasse e contributi, pagamenti, rimborsi, agevolazioni/borse); dati relativi a servizi agli studenti (es. tutorato, supporto, placement); dati di accesso a piattaforme e servizi digitali (credenziali, identificativi e log tecnici nei limiti applicabili);

2) Ambito del personale

(Selezione, formazione, gestione economica, giuridica e previdenziale del personale; protezione e prevenzione sul luogo di lavoro, ecc.)

A titolo esemplificativo, l'Università tratta: dati anagrafici e di contatto; dati identificativi e fiscali; dati relativi a selezione e reclutamento (CV, titoli, esiti); dati contrattuali e di carriera (qualifica, ruolo, incarichi, progressioni); dati amministrativi e giuslavoristici (presenze/assenze, ferie, permessi); dati retributivi, contributivi e bancari (paghe, rimborsi, coordinate); dati formativi (corsi svolti/obbligatori); dati necessari alla gestione della sicurezza sul lavoro e degli obblighi di prevenzione/protezione, nei limiti applicabili; dati per l'abilitazione e la gestione degli accessi a sistemi informativi e risorse (credenziali, profili, log tecnici).

3) Ambito economico-finanziario

(Contabilità, fatturazione attiva e passiva, recupero crediti, approvvigionamenti, ecc.)

A titolo esemplificativo, l'Università tratta: dati identificativi e di contatto di fornitori, professionisti, referenti e controparti; dati fiscali, amministrativi e bancari (codici fiscali/P.IVA, IBAN, estremi di pagamento); dati contrattuali (ordini, convenzioni, contratti, capitolati); dati contabili e di fatturazione (fatture, note, scadenze, rendicontazioni); dati relativi a procedure di acquisto e gare, ove previste; dati relativi a gestione crediti/debiti e attività di recupero; dati connessi a contenzioso, reclami o verifiche ispettive/di compliance.

4) Ambito comunicazione (comunicazione istituzionale e brand management)

(Promozione attività universitarie e didattiche, attività post-lauream, reperimento fondi, adesione a iniziative, ecc.)

A titolo esemplificativo, l'Università tratta: dati identificativi e di contatto di utenti/contatti (es. studenti potenziali, alumni, partecipanti ad iniziative, sponsor/partner); dati relativi a iscrizioni e partecipazioni a eventi, webinar, open day e iniziative; immagini e contenuti audio-video raccolti durante eventi/attività di comunicazione; dati relativi a campagne di raccolta fondi e adesioni a iniziative; dati tecnici di navigazione e fruizione dei canali web (es. cookie e

strumenti analoghi).

5) Ambito attività operative

(Gestione della videosorveglianza e controllo accessi)

A titolo esemplificativo, l'Università tratta: immagini e riprese video; dati relativi a accessi e transiti (es. badge, identificativi, varchi, registri accessi), nonché informazioni tecniche connesse al funzionamento dei sistemi (log) nei limiti applicabili; eventuali dati identificativi associati a credenziali/abilitazioni di accesso alle sedi e alle risorse.

6) Attività di ricerca scientifica

(Ricerca scientifica e sperimentazioni cliniche in ambito medico-biomedico ed epidemiologico)

A titolo esemplificativo, l'Università tratta: dati anagrafici e di contatto dei partecipanti, ove necessari; dati relativi a arruolamento e gestione dello studio; dati clinici e sanitari, dati genetici e/o biometrici ove previsti dai protocolli; dati relativi a esami, referti, parametri, anamnesi e follow-up; dati raccolti tramite dispositivi/strumentazioni e piattaforme di ricerca; codici identificativi.

7.1 Trattamento di categorie particolari di dati personali e di dati relativi a condanne penali e reati (artt. 9 e 10 del Regolamento)

Il trattamento dei dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dei dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento sessuale delle persone fisiche, è vietato, salvo che ricorrano le condizioni di liceità previste dall'articolo 9 del Regolamento.

L'Università, in qualità di Titolare del trattamento, può trattare tali dati solo nei casi espressamente previsti dal Regolamento, e segnatamente quando il trattamento:

- è fondato sul consenso esplicito dell'interessato per una o più finalità determinate, ove tale consenso non sia escluso dalla normativa nazionale o dell'Unione;
- è necessario per l'adempimento di obblighi o l'esercizio di diritti del Titolare o dell'interessato in materia di diritto del lavoro, sicurezza sociale o protezione sociale, nei limiti consentiti dal diritto dell'Unione o nazionale, e in presenza di garanzie adeguate per i diritti e gli interessi dell'interessato;
- è indispensabile per tutelare un interesse vitale dell'interessato o di altra persona fisica, qualora l'interessato si trovi nell'impossibilità fisica o giuridica di prestare il proprio

consenso;

- è effettuato, con adeguate garanzie, da enti, fondazioni o associazioni senza scopo di lucro che perseguano finalità politiche, filosofiche, religiose o sindacali, limitatamente ai dati dei propri membri o contatti abituali, e senza comunicazione esterna senza consenso;
- riguarda dati personali resi manifestamente pubblici dall'interessato;
- è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, o quando le autorità giurisdizionali esercitino le proprie funzioni;
- è giustificato da motivi di interesse pubblico rilevante, sulla base del diritto dell'Unione o degli Stati membri, in modo proporzionato alla finalità perseguita e accompagnato da misure adeguate di tutela dei diritti e delle libertà degli interessati;
- è necessario per finalità sanitarie, quali la diagnosi, l'assistenza, la terapia, la medicina preventiva o la gestione dei servizi sanitari e sociali, sulla base del diritto dell'Unione o nazionale o di un contratto con un professionista della sanità, nel rispetto delle condizioni di riservatezza e del segreto professionale;
- è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce sanitarie transfrontaliere o la garanzia di elevati standard di sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici, sulla base di disposizioni che assicurino adeguate garanzie e il rispetto del segreto professionale;
- è effettuato per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89 del Regolamento e alla normativa nazionale applicabile, con l'adozione di misure tecniche e organizzative atte a tutelare i diritti e le libertà degli interessati.

Il trattamento dei dati personali relativi a condanne penali, reati o a connesse misure di sicurezza è disciplinato dall'articolo 10 del Regolamento e può essere effettuato solo sotto il controllo di un'autorità pubblica o se è autorizzato dal diritto dell'Unione o nazionale, purché siano previste garanzie adeguate alla tutela dei diritti e delle libertà degli interessati.

Eventuali registri completi delle condanne penali sono tenuti esclusivamente 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.

L'Università tratta dati di cui all'art. 9 e all'art. 10 del Regolamento solo qualora il trattamento

sia necessario per lo svolgimento delle proprie attività istituzionali e non sia possibile perseguire le medesime finalità mediante il trattamento di dati anonimi o di dati personali comuni. 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 agli artt. 9 e 10 del Regolamento contenuti in banche dati trattate con mezzi elettronici è necessario utilizzare tecniche di cifratura, 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 sopra anche quando sono tenuti in elenchi, registri, banche dati senza l'utilizzo di strumenti elettronici.

ART. 8 – MISURE DI SICUREZZA

I dati personali oggetto di trattamento sono gestiti e custoditi con modalità tali da assicurare un livello di protezione adeguato rispetto alla natura delle informazioni, alle caratteristiche delle operazioni compiute e al progresso tecnico in materia di sicurezza.

Attraverso l'adozione di misure di sicurezza preventive e proporzionate, l'Università garantisce che siano ridotti al minimo i rischi di distruzione o perdita, anche accidentale, di accesso o comunicazione non autorizzati, nonché di trattamenti non consentiti o non conformi alle finalità per le quali i dati sono stati raccolti.

Per tutti i trattamenti, prima della loro esecuzione, viene valutato il livello di rischio ed effettuata, se il trattamento presenta rischi elevati per i diritti e le libertà degli interessati, la valutazione d'impatto sulla protezione dei dati ("DPIA" o "*Data Protection Impact Assessment*") ai sensi dell'articolo 35 del Regolamento, individuando opportune misure organizzative e tecniche per la messa in sicurezza dei dati. Qualora le misure aggiuntive dedotte nella valutazione d'impatto 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).

L'Università esegue con regolarità, anche con il supporto di società specializzate nell'ambito della *cybersecurity*, sessioni di *vulnerability assessment* e di *penetration test* al fine di

individuare tempestivamente eventuali vulnerabilità dei sistemi e prevenire fenomeni di compromissione o violazioni dei dati personali.

Inoltre, sono implementate procedure strutturate di gestione e protezione dei dati, sostenute da sistemi tecnologici di backup e di ripristino, volti a garantire la continuità operativa e l'immediato recupero delle informazioni in caso di eventi che possano compromettere la disponibilità o l'integrità degli archivi.

L'Università si accerta, prima della messa in opera di piattaforme applicative complesse, che esse siano conformi alla legislazione nazionale e sovranazionale per quanto attiene il trattamento e la protezione dei dati personali.

L'Ateneo provvede a nominare gli amministratori di sistema in conformità al 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 atto il relativo sistema di "Log delle attività degli amministratori di sistema".

È stata adottata un'istruzione operativa "*Richiesta e uso delle risorse informatiche*" pubblicata sulla intranet aziendale, che disciplina l'uso delle apparecchiature e dei dispositivi elettronici messi a disposizione dall'Ateneo, nonché di quelli personali eventualmente impiegati dal personale dipendente o collaboratore. Il documento disciplina, altresì, le modalità di connessione alle reti locali, incluse le reti Wi-Fi e geografiche, e l'utilizzo della posta elettronica.

Il personale e gli studenti dell'Ateneo possono utilizzare strumentazione informatica messa a disposizione dall'Ateneo; strumentazione informatica propria (computer portatile) previa autorizzazione dell'Area Sistemi informativi, nel rispetto del Codice Etico di Ateneo e delle specifiche procedure interne. In particolare, la strumentazione informatica messa a disposizione del personale dell'Università dovrà essere utilizzata in conformità delle norme riportate nel documento "*Richiesta e uso delle risorse informatiche*" 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.

L'Università si avvale di un sistema strutturato di autenticazione e di autorizzazione all'accesso, volto a garantire la protezione dei dati personali, in particolare di quelli appartenenti a categorie particolari di cui all'articolo 9 del Regolamento, e a prevenire qualunque forma di accesso

indebito o trattamento non autorizzato. Il Titolare assicura che solo i soggetti formalmente designati e autorizzati al trattamento possano accedere alle informazioni, evitando ogni rischio di comunicazione, diffusione, alterazione o utilizzo non conforme alle finalità istituzionali.

I Referenti interni e tutti gli incaricati/Autorizzati al trattamento sono impegnati al rispetto delle misure di sicurezza tecniche e organizzative definite dal Titolare.

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 delle attività di trattamento consentite ai singoli incaricati/Autorizzati al trattamento e agli 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 delle attività di trattamento consentite ai singoli incaricati/Autorizzati al trattamento;
2. previsione di istruzioni finalizzate ad un'adeguata custodia di atti e documenti cartacei affidati agli Autorizzati al trattamento per lo svolgimento dei relativi compiti;
3. previsione di procedure finalizzate alla conservazione di determinati atti in archivi ad accesso protetto e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il DPO e il Responsabile della Direzione Sistemi Informativi garantiscono un servizio di supporto e di verifica per tutto ciò che riguarda la sicurezza dei trattamenti di dati personali e i connessi adempimenti previsti dal Regolamento UE e dal presente Modello.

ART. 9 – COMUNICAZIONE DEI DATI PERSONALI A SOGGETTI ESTERNI ALL'UNIVERSITÀ

Ferme restando: (i) la comunicazione di dati personali a soggetti formalmente designati Responsabili del trattamento ai sensi dell'art. 28 GDPR, nei limiti e per le finalità previste dallo specifico atto di nomina; nonché (ii) la comunicazione a soggetti terzi lecita e necessaria per l'esecuzione di uno specifico rapporto in essere con l'interessato (e coerente con le finalità dichiarate e la base giuridica del trattamento), ogni ulteriore richiesta volta a ottenere la comunicazione o la diffusione di dati personali deve essere formalizzata per iscritto dall'Incaricato coinvolto nel trattamento e/o dal Referente interno della Direzione/Area/Servizio/Ufficio/Unità Operativa competente, che provvede tempestivamente a informare il DPO.

In ogni caso, l'Incaricato/persona autorizzata non è autorizzata a procedere autonomamente alla comunicazione o diffusione dei dati e deve inoltrare senza indugio la richiesta secondo i canali indicati. Il DPO, ricevuta la richiesta, valuta la legittimità della comunicazione/diffusione (base giuridica, finalità, pertinenza e minimizzazione, eventuali vincoli di riservatezza, misure di sicurezza e tracciabilità) e fornisce il relativo parere e supporto alle strutture competenti per le determinazioni conseguenti.

9.1 Richieste provenienti da soggetti pubblici

La comunicazione di dati personali su richiesta di soggetti pubblici è ammessa quando:

- è prevista da una norma di legge o di regolamento; oppure
- in mancanza di una previsione espressa, è necessaria per lo svolgimento di funzioni istituzionali dell'ente pubblico richiedente; oppure
- la richiesta proviene dall'Autorità giudiziaria o da Autorità/Organi di pubblica sicurezza, nei limiti e con le modalità previste dalla normativa applicabile.

9.2 Richieste provenienti da soggetti privati

Le richieste provenienti da soggetti privati possono essere accolte solo se fondate su una specifica base normativa (legge, regolamento o atti normativi speciali) e devono essere adeguatamente motivate. La richiesta deve contenere almeno:

- nome, denominazione o ragione sociale del richiedente e relativi riferimenti;
- indicazione dei dati oggetto di richiesta;
- finalità del trattamento e modalità di utilizzo dei dati richiesti, inclusa l'eventuale ulteriore comunicazione a terzi.

9.3 Divieti e limitazioni

La comunicazione e/o diffusione dei dati personali è in ogni caso vietata, oltre che nei casi di divieto disposto dall'Autorità di controllo o dall'Autorità giudiziaria:

- con riferimento a dati personali per i quali sia stata disposta la cancellazione ovvero quando sia decorso il termine di conservazione previsto;
- con riferimento a dati personali rispetto ai quali l'interessato abbia validamente esercitato i diritti di cancellazione, limitazione o opposizione, nei limiti e per gli effetti previsti dal GDPR;
- per finalità diverse o incompatibili rispetto a quelle indicate nelle informative e, ove richiesto, rispetto a quelle per cui è stato acquisito il consenso.

È fatta salva la comunicazione o diffusione effettuata, in conformità alla legge, su richiesta delle forze di polizia, dell'Autorità giudiziaria, degli organismi di informazione e sicurezza o di altri soggetti pubblici competenti, per finalità di difesa o sicurezza dello Stato ovvero di prevenzione, accertamento o repressione dei reati.

Nel rispetto dei principi di liceità, minimizzazione e proporzionalità, nonché in coerenza con i fini istituzionali dell'Università, può ritenersi di norma lecita la comunicazione di dati personali relativi a studenti e laureati a soggetti pubblici o privati e a consorzi interuniversitari che ne facciano richiesta per finalità connesse all'orientamento, alla formazione e all'inserimento professionale, ivi inclusa la partecipazione a incontri, manifestazioni, riunioni o congressi, previa valutazione del DPO e nel rispetto delle basi giuridiche e delle garanzie applicabili.

ART. 10 – 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 un'apposita informativa che renda nota al pubblico la 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 all'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 relative ai trattamenti di dati personali posti in essere attraverso i sistemi di videosorveglianza adottati dall'Ateneo sono descritte all'interno delle specifiche informative rese ai sensi dell'art. 13 GDPR al personale dipendente e ai visitatori dei locali dell'Università, sia in versione estesa sia in versione breve tramite apposita cartellonistica affissa nei locali universitari.

L'Università ha nominato un Referente interno specificatamente autorizzato al trattamento dei dati personali raccolti con il sistema di videosorveglianza, a cui sono state fornite istruzioni precise per l'accesso alle immagini.

Tale soggetto tiene traccia delle richieste di accesso e/o blocco temporaneo delle immagini mediante un *Registro delle richieste* in formato Excel.

Rispetto al trattamento dei dati personali acquisiti tramite il sistema di videosorveglianza, l'Università agisce in qualità di Titolare del trattamento nel rispetto del Regolamento e della normativa nazionale applicabile, nonché delle garanzie previste dall'art. 4 della L. 300/1970 ("Statuto dei Lavoratori") e delle ulteriori tutele poste a protezione dei lavoratori.

L'attivazione e l'impiego del sistema sono stati oggetto di specifica autorizzazione da parte dell'Ispettorato Territoriale del Lavoro (ITL), nel rispetto delle procedure autorizzative ex art. 4, co. 1, dello Statuto dei Lavoratori, e sono stati preceduti da una valutazione d'impatto sulla protezione dei dati (DPIA), finalizzata a verificare e mitigare i rischi per i diritti e le libertà degli interessati e a definire le misure tecniche e organizzative applicabili.

La visualizzazione, la trasmissione e l'utilizzo delle immagini raccolte possono avvenire esclusivamente per le finalità legittime individuate e comunicate agli interessati nelle informative rese, nel rispetto dei principi di necessità, proporzionalità e minimizzazione, nonché delle misure di sicurezza adottate e dei limiti e prescrizioni derivanti dall'autorizzazione rilasciata dall'ITL e dalla disciplina applicabile.

ART. 11 – TRASFERIMENTO DI DATI ALL'ESTERO PER ATTIVIT 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 fuori dallo Spazio Economico Europeo (SEE).

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 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.

A tal fine, il DPO, in tutte le situazioni in cui nell'ambito del rapporto contrattuale ravvisi un trasferimento di dati personali verso un paese fuori dallo Spazio Economico Europeo in cui l'Ateneo rivesta il ruolo di esportatore di dati, sulla base di quanto indicato nella *Policy sul trasferimento dei dati fuori dallo spazio SEE,* dovrà fare riferimento alle indicazioni utili sui principi applicabili ai trasferimenti di dati personali fuori dallo Spazio Economico Europeo, nonché sulle condizioni di liceità per effettuare tale trasferimento nel rispetto della normativa di riferimento in materia.

Più in particolare, tale policy prevede le seguenti istruzioni:

- In primis occorre verificare se l'importatore risiede in un paese per il quale sia stata adottata una decisione di adeguatezza consultando l'elenco aggiornato pubblicato sul sito web della Commissione Europea, al seguente link: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions.

  Se l'importazione dei dati è verso gli **Stati Uniti**, occorre verificare sul sito web del Data Privacy Framework (https://www.dataprivacyframework.gov/s/.) se il destinatario negli Stati Uniti è certificato e se il trasferimento dei dati pertinenti sia coperto da tale certificazione.
- In difetto, occorre verificare la sussistenza di un'altra condizione di legittimità per il trasferimento dei dati. Se si ritiene di far ricorso alle clausole contrattuali tipo o standard di protezione dei dati, adottate dalla Commissione Europea, occorre scegliere tra i quattro modelli di clausole in base all'inquadramento privacy individuato:
  - trasferimenti da Titolare a Titolare;

- trasferimenti da Titolare a Responsabile;
- trasferimenti da Responsabile a Responsabile;
- trasferimenti da Responsabile a Titolare;

Oltre a richiedere copia firmata delle Clausole Contrattuali Standard, quando l'Ateneo utilizza i modelli di Clausole Contrattuali Standard "Titolare a Titolare" o "Titolare a Responsabile" deve svolgere anche una o più valutazioni di impatto sulla legislazione del luogo di trasferimento (cd. Transfer Impact Assessment o "TIA", "DTIA") ai sensi della Clausola 14 delle Clausole Contrattuali Standard adottate dalla Commissione Europea.

All'esito, il DPO procederà alla registrazione del trasferimento di dati personali all'interno del Registro dei trattamenti, ex art. 30 GDPR, riportando i paesi terzi od organizzazioni internazionali a cui i dati personali sono stati o saranno comunicati, la valutazione del rischio effettuata e la descrizione delle garanzie attuate per il trasferimento, in relazione ai rischi valutati (ciò affinché l'interessato benefici di un adeguato livello di protezione dei suoi dati personali sia nel trasferimento dei dati verso un paese terzo sia nell'eventuale ulteriore trasferimento da questi ad altro paese terzo, secondo le disposizioni del Capo V del GDPR).

ART. 12 – ATTIVITÀ NELL'AMBITO DELLA RICERCA SCIENTIFICA

L'Università e la Fondazione Policlinico Universitario Campus Bio-Medico ("Fondazione") hanno stipulato una Convenzione che ha lo scopo 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 Regolamento), 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. 13 - 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.

13.1 Presenza di studenti nei percorsi di cura presso la Fondazione per attività formative

Lo svolgimento delle attività formative professionalizzanti rivolte a studenti tirocinanti e specializzandi prevede, in occasione dell'erogazione delle prestazioni sanitarie da parte del professionista sanitario presso la Fondazione a favore dei pazienti, la partecipazione e il coinvolgimento degli studenti iscritti ai corsi di laurea e post-laurea presso l'Università, come da Convenzione in essere tra l'Ateneo e la Fondazione. 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. 14 – AMBITO DI RESPONSABILITÀ

All'interno dell'Università, chiunque riceva, tratti o richieda dati personali è vincolato al dovere di riservatezza ed è tenuto ad adottare tutte le misure necessarie a garantirne la sicurezza e la protezione contro accessi non autorizzati.

La responsabilità, anche di natura penale, come prevista dall'ordinamento nazionale, per l'utilizzo illecito dei dati personali e non conforme alle istruzioni impartite dal Titolare del trattamento, ricade esclusivamente sul soggetto cui tale uso illecito 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.

ART. 15 – NORMA FINALE

Per quanto non previsto nel presente Regolamento interno per la protezione dei dati personali, si applicano le disposizioni normative del Regolamento, 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 annuale.