Università San Raffaele Roma

MODELLO ORGANIZZATIVO PRIVACY (MOP) DI

UNIVERSITÀ TELEMATICA SAN RAFFAELE ROMA S.R.L.

AI SENSI DEL REGOLAMENTO EUROPEO 2016/679

Allegato 1 del Modello Organizzativo Privacy

General Data Privacy Policy

EDIZIONE N. 3

INDICE DELLA GENERAL DATA PRIVACY POLICY

1. INTRODUZIONE

1.1. SCOPO

Lo scopo del presente documento è quello di indicare la politica adottata da **Università Telematica San Raffaele Roma S.r.l.** (di seguito anche "*Università"* o *"UTSR"*) per regolare le modalità e i principi da seguire durante le operazioni di trattamento dei dati personali al fine di assicurare un adeguato e idoneo standard di sicurezza nel rispetto della vigente normativa come disciplinata dal Regolamento (UE) 2016/679.

Con l'osservanza di questo documento s'intende richiamare l'attenzione di tutte le risorse operanti all'interno o per conto dell'Università al rispetto della normativa sulla sicurezza dei dati personali, con espressa attenzione all'impiego delle risorse cartacee, informatiche e del sistema di videosorveglianza utilizzati.

All'interno della presente Policy sono indicate le procedure per l'utilizzo delle banche dati informatiche e/o cartacee che costituiscono patrimonio aziendale e che sono, come tali, soggette alla proprietà e al controllo del Titolare del trattamento.

Il presente documento costituisce, dunque, un disciplinare vincolante per il personale dipendente e somministrato, inclusi gli stagisti ed i tirocinanti (c.d. *"dipendenti"*) dell'UTSR, operante presso tutte le sedi e/o fuori di esse (anche attraverso la modalità di lavoro in smart working o di telelavoro).

1.2. APPLICABILITÀ

Il presente documento si applica all'Università ed è rivolta a tutti i dipendenti e collaboratori esterni, intesi come fornitori di servizi, terze parti, outsourcers, liberi professionisti, che, a diverso titolo e per diversi scopi, collaborano con l'Università, effettuando attività di trattamento di dati personali.

2. RIFERIMENTI NORMATIVI

[Rif. 1] ➔ Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). Per *"GDPR"* si intende *"General Data Protection Regulation"*.

[Rif. 2]➔ Provvedimenti del Garante *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"* (G.U. n. 300 del 24 dicembre 2008) e successive modifiche ed integrazioni.

[Rif. 3] ➔ Codice Privacy: D.lgs. 196/03 come modificato dal D.lgs. 101/18.

3. ACRONIMI E DEFINIZIONI

Acronimi e definizioni	Descrizione
MOP	Modello Organizzativo Privacy.
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.
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.
Dato particolare	Il dato personale che si riferisce a categorie di informazioni sensibili, quali quelle riguardanti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici e biometrici diretti a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita e/o all'orientamento sessuale della persona, dati relativi a condanne penali e reati.
Dato genetico	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.
Dato biometrico	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o

Acronimi e definizioni	Descrizione
	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.
Dati giudiziari	Dati personali relativi a condanne penali e reati, o connessi a misure di sicurezza.
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.
Designato *interno* del trattamento	Il soggetto interno all'organizzazione aziendale che opera sotto l'autorità del Titolare del trattamento, al quale quest'ultimo può, sotto la propria responsabilità, affidare specifici compiti connessi alle operazioni di trattamento dei dati personali.
Autorizzato al trattamento	La persona fisica che, previa specifica autorizzazione del Titolare o del Designato nominato dal Titolare, elabora e utilizza materialmente dati personali sulla base delle istruzioni ricevute dai medesimi soggetti e sotto la loro autorità diretta.
Interessato	La persona fisica alla quale si riferiscono i dati personali oggetto di trattamento, cui spetta l'esercizio dei diritti accordati dal Reg. UE 16/679.
Responsabile del trattamento ex art. 28 Reg. UE 16/679	La persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, previa specifica designazione, tratta dati personali per conto del Titolare del trattamento.
Destinatario	La persona fisica o giuridica, l'Autorità pubblica o un altro organismo, che riceve comunicazione di dati personali, che si tratti o meno di terzi.
Terzi	La persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che non sia il Titolare, il Responsabile ex art. 28 Reg. UE 16/679 o le persone autorizzate al trattamento dei dati personali, sotto la diretta autorità del Titolare o del Responsabile ex art. 28 Reg. UE 16/679.

Acronimi e definizioni	Descrizione
Organizzazione internazionale	Organizzazione o altri 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.
Atto di nomina	Il documento attraverso il quale il Titolare o il Designato nominato del Titolare nominano e autorizzano la persona al trattamento di dati personali, individuandone le istruzioni e l'ambito consentito in base alla mansione svolta.
Informativa	Complesso di informazioni fornite dal Titolare del trattamento ad ogni Interessato, quando i dati sono raccolti presso il medesimo o presso terzi, finalizzate a fornire in modo trasparente ed intellegibile specifiche indicazioni, previste inderogabilmente dall'art. 13 Reg. UE 16/679, indispensabili all'Interessato, anche al fine di poter esercitare consapevolmente i propri diritti relativi ai dati personali.
Consenso	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, a che i dati personali che lo riguardano siano oggetto di trattamento.
IT	Information Technology, le tecnologie dell'informazione.
Hardening	Procedure di sicurezza di un sistema, mirate al restringimento dei soli servizi necessari e alla modifica delle impostazioni di *"default"*.
OS	Operating System (Sistema operativo).
Credenziali di autenticazione	Credenziali e password attribuite alla persona autorizzata al trattamento all'atto dell'assunzione, e della contestuale nomina ad Autorizzato, per poter accedere ai sistemi messi a disposizione dall'Università in base alla mansione svolta.
Area di appartenenza	L'ufficio dove ciascuna persona autorizzata presta la propria attività lavorativa.
Misure adeguate di	Misure idonee dirette a ridurre al minimo i rischi di distruzione e perdita, anche accidentale, di accesso non autorizzato o di

Acronimi e definizioni	Descrizione
sicurezza	trattamento non consentito o non conforme alle finalità per cui sono stati raccolti i dati personali.
DB	Data Base (Banca dati).
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.
Pseudonimizzazione	Procedura volta al mascheramento di dati personali in modo che essi 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.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per prevedere o analizzare 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.
Data breach	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.
DPIA	Data Protection Impact Assessment (Valutazione d'impatto sulla protezione dei dati). È una procedura di analisi che mira a valutare la necessità, la proporzionalità ed i rischi di un trattamento, allo scopo di approntare misure idonee e adeguate ad affrontarli e gestirli.
Sanzioni	In caso di inottemperanza alla disciplina e alle disposizioni del Reg. UE 16/679 è prevista l'applicazione di sanzioni pecuniarie amministrative fino a € 20 milioni o al 4% del fatturato annuale

Acronimi e definizioni	Descrizione
	globale, nonché di sanzioni penali, qualora la violazione integri un reato di quelli previsti dal Reg. UE 16/679, dal D.lgs. 196/03, dal D.lgs. 101/18.

4. PRINCIPI GENERALI

La progressiva diffusione delle nuove tecnologie informatiche espone l'Università al rischio di un coinvolgimento in forme di responsabilità di tipo amministrativo, civile e addirittura penale.

Eventuali problematiche inerenti alla sicurezza della protezione dei dati (personali, ma anche aziendali) potrebbero avere, pertanto, ripercussioni dannose per l'Università sia dal punto di vista reputazionale che patrimoniale.

È proprio al fine di evitare il verificarsi di simili ipotesi, ed allo specifico scopo di assicurare l'adeguata protezione di tutti i dati trattati dall'Università ivi compresi quelli conservati in banche dati non automatizzate, che l'Università ha ritenuto doveroso, con riferimento specifico alle misure di sicurezza imposte per il trattamento dei dati personali dal Reg. UE 2016/679, formalizzare idonee indicazioni ed istruzioni per tutto il personale interessato.

Premesso, quindi, che il trattamento dei dati e l'utilizzo dei dati da parte dell'Università, attraverso modalità e risorse informatiche e non, rientra nell'ambito del rapporto di lavoro e che lo stesso deve ispirarsi al principio della diligenza, della correttezza e dell'osservanza della normativa vigente, è stata delineata la presente Policy diretta a evitare che comportamenti anche solo inconsapevoli possano innescare condizioni di incertezza o di minaccia alla sicurezza nel trattamento dei dati e/o integrare fattispecie di rilevanza civile e amministrativo-penale.

Nell'ambito della gestione dei processi di protezione dei dati e delle informazioni trattate, l'Università garantisce il rispetto dei seguenti principi generali:

1. **Liceità, correttezza e trasparenza**: le operazioni di trattamento devono essere condotte in maniera chiara, corretta e trasparente nei confronti dell'Interessato. In tal senso assume rilevanza redigere delle Informative chiare, intelligibili, corrette e complete da trasmettere all'Interessato, individuare correttamente la base giuridica posta alla base del trattamento nonché la corrispondenza tra il trattamento e le finalità stabilite all'interno delle Informative stesse.

   Ciò significa che per effettuare operazioni di trattamento sui dati personali in modo corretto e trasparente risulterà primario individuare all'interno delle Informative una delle seguenti basi giuridiche:

   - l'Interessato ha prestato il proprio consenso;
   - il trattamento è necessario per l'esecuzione di un contratto o di misure precontrattuali con la risorsa interessata;
   - adempimento di obblighi legali;

- proteggere gli interessi vitali dell'Interessato;
- perseguire i legittimi interessi del Titolare del trattamento per altre finalità quando non prevalgono gli interessi o i diritti e le libertà fondamentali degli Interessati al trattamento. Qualora si facesse ricorso ai *"legittimi interessi"* per trattare dati personali, occorre chiaramente spiegare il tipo di interesse nella relativa Informativa sulla Privacy.

2. **Esattezza ed aggiornamento**: occorre accertare che i dati personali utilizzati e conservati siano corretti, completi, aggiornati. Pertanto, è necessario mantenere un presidio di controllo sulla correttezza dei dati al momento della raccolta e, successivamente, a intervalli regolari. I dati personali non corretti o non aggiornati devono essere distrutti o modificati entro un ragionevole lasso di tempo dal momento in cui emerge l'errore (ad es. entro 72 ore dalla notifica dell'errore da parte di un cliente o un dipendente).

3. **Limitazione della finalità**: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati per perseguire le finalità per le quali sono stati raccolti. Questo implica che non si ha la facoltà di utilizzare dati personali per finalità nuove, differenti o incompatibili da quella comunicata attraverso l'Informativa o quando è stato ottenuto il consenso (eccetto nei casi in cui la persona sia stata opportunamente informata circa le nuove finalità e che abbia rilasciato il relativo consenso, laddove necessario). Per esempio, se vengono raccolti dati personali relativi a un/a candidato/a ai fini di una assunzione, non sarà possibile utilizzare tali dati per finalità differenti che siano incompatibili con l'assunzione stessa dell'Interessato (ad esempio l'invio di materiale pubblicitario).

4. **Integrità e riservatezza**: i dati personali devono essere trattati in modo tale da garantire un'idonea e adeguata sicurezza per i medesimi durante le operazioni di trattamento. Il Reg. UE 16/679 precisa che un livello idoneo di sicurezza si può ottenere mediante l'adozione misure tecniche e organizzative adeguate e commisurate al rischio (art. 32), atte ad evitare che vengano attuati trattamenti non autorizzati o illeciti, nonché che si possa configurare la perdita, la divulgazione non autorizzata, la distruzione e qualsiasi altro nocumento, anche accidentale, ai dati personali.

5. **Limitazione della conservazione**: i dati personali devono essere conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per cui vengono trattati.

   È vietato conservare dati personali in una forma che consenta l'identificazione della persona per un tempo superiore a quanto necessario per la finalità per le quali sono stati raccolti, ivi compresa quella di soddisfare eventuali requisiti di carattere legale, contabile o di reportistica.

   Infine, occorre accertarsi che gli Interessati siano informati circa il periodo di conservazione dei dati e le relative modalità di calcolo dei tempi all'interno della relativa Informativa sulla Privacy.

6. **Limitazione al trasferimento in Paese terzo**: possibile solo previa adozione e riscontro di misure di protezione adeguate.

Il Reg. UE 16/679 limita il trasferimento di dati ai Paesi al di fuori dell'Area Economica Europea (che comprende i 28 paesi dell'UE, l'Islanda, il Liechtenstein e la Norvegia) ("AEE") per assicurare che non venga meno il livello di protezione dei dati offerto agli Interessati dal Reg. UE 16/679 stesso.

Si ha la facoltà di trasferire i dati personali al di fuori dell'AEE unicamente se sussiste una delle seguenti condizioni:

- la Commissione Europea ha emesso una decisione che conferma che il paese in cui vengono trasferiti i dati personali assicura un adeguato livello di protezione per i diritti e le libertà della persona;
- esistono sistemi di protezione adeguati, come norme vincolanti d'impresa, clausole contrattuali standard approvate dalla Commissione Europea, un codice deontologico o meccanismo di certificazione approvato;
- la persona ha dato il suo consenso esplicito al trasferimento proposto dopo essere stata informata dei potenziali rischi;
- il trasferimento è necessario per una delle altre ragioni definite nel Reg. UE 16/679, compresa l'esecuzione di un contratto tra l'Università e la persona, per ragioni di pubblico interesse, per istituire, esercitare azioni legali o per proteggere gli interessi vitali della persona, laddove questo sia fisicamente o legalmente incapace a dare il proprio consenso e, in casi più rari, per il legittimo interesse dell'Università stessa.

Occorre rammentare che, se il trasferimento di dati transfrontaliero avviene nell'ambito della collaborazione con una parte terza (ad esempio mentre è in uso un sistema informatico che si trova al di fuori del SEE), sarà necessario rispettare i requisiti in termini di coinvolgimento delle parti terzi chiamate a trattare dati personali per conto dell'Università.

7. **Privacy by design**: devono essere messe in atto, al momento di determinare i mezzi del trattamento ed all'atto del trattamento stesso, misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento [Rif.1] e tutelare i diritti degli Interessati.

8. **Minimizzazione***:* i dati personali raccolti devono essere adeguati, pertinenti e limitati rispetto alle finalità stabilite. Raccogliere un numero eccessivo di dati, anche superflui rispetto alle finalità perseguite, costituisce un rischio per l'organizzazione aziendale in quanto più dati si raccolgono, più dati dovranno essere gestiti e protetti. Occorre, quindi, assicurare che:
   - i dati personali raccolti siano adeguati e pertinenti alle finalità per cui sono stati raccolti;
   - una volta che i dati personali non sono più necessari per finalità specifiche, siano cancellati o resi anonimi in conformità con le linee guida sulla conservazione dei dati.

9. **Privacy by default:** devono essere messe in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per

ogni specifica finalità del trattamento. Tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Una *"misura tecnica"* comprende misure tramite sistemi tecnologici come protezione della password, criptazione, sistemi di rilevazione delle intrusioni e firewall.

Una *"misura organizzativa"* è qualsiasi misura implementata da un'organizzazione al fine di proteggere i dati personali che non siano necessariamente di natura tecnologica quali, ad esempio, le politiche, le procedure e la formazione erogata.

In tal senso risulterà opportuno effettuare una valutazione periodica di tali misure al fine di accertare che siano costantemente idonee in relazione alla natura dei dati personali trattati.

10. **Need to Know**: assegnazione dell'utenza di accesso ad un sistema/servizio informatico esclusivamente agli utenti che necessitano dell'accesso a tale sistema/servizio per lo svolgimento delle proprie attività lavorative.
11. **Least Privilege**: assegnazione a ciascun utente di un set di privilegi minimo necessario per l'espletamento delle proprie attività lavorative.
12. **Segregation of Duty**: scomposizione delle responsabilità, dei compiti e dei privilegi tra più utenti al fine di garantire che un dato processo non sia controllato interamente da un singolo soggetto e in modo da ridurre i rischi connessi ad abusi ed errori.
13. **Defense in depth**: il principio stabilisce che devono essere previsti dei controlli di sicurezza in ognuno degli strati dell'architettura (i.e. network, application, OS e DB); lo sviluppo di controlli di sicurezza in tutti gli strati dell'architettura fa in modo che la compromissione della sicurezza in un singolo strato non sia sufficiente a compromettere l'intera architettura.
14. **Riservatezza**: solo gli utenti autorizzati possono decifrare l'informazione e nessun soggetto terzo può accedere al contenuto informativo, anche se in possesso dell'informazione cifrata.
15. **Integrità**: il contenuto informativo non può essere alterato ed è possibile verificare l'integrità delle informazioni al fine di stabilire l'occorrenza di una qualunque alterazione.
16. **Disponibilità**: il contenuto informativo deve essere sempre disponibile e fruibile quando viene richiesto.
17. **Responsabilizzazione (accountability)**: onere probatorio a carico del Titolare del trattamento circa il rispetto di tutti i principi previsti dal GDPR nell'attività di trattamento dei dati personali.
18. **Diritti e richieste degli Interessati al trattamento**: il Titolare del trattamento ha l'onere di rendere possibile e facilmente fruibile l'esercizio degli specifici diritti riconosciuti dal Reg. UE 16/679 agli Interessati rispetto ai loro dati personali.

    Tra i diritti, ci sono quelli inerenti alla possibilità di:

    - **revocare** il consenso al trattamento in qualsiasi momento;

- esercitare il **diritto di accesso** ex art. 15 Reg. UE 16/679 ai dati personali in possesso dell'Università, ottenendo dal Titolare la conferma che sia in corso un trattamento di dati personali che lo riguardano e di ottenere l'accesso ai dati personali e alle seguenti informazioni: finalità, categorie di dati personali, i destinatari o le categorie di destinatari, il periodo di conservazione, l'esistenza di altri diritti previsti dal GDPR, il diritto di proporre reclamo al Garante della Privacy, l'esistenza di un processo automatizzato di profilazione ecc.;
- esercitare il **diritto di rettifica** ex art. 16 Reg. UE 16/679 ottenendo dal Titolare la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo;
- esercitare il **diritto alla cancellazione** dei dati ex art. 17 Reg. UE 16/679 richiedendo al Titolare la cancellazione dei dati personali se non più necessari rispetto alle finalità per i quali sono stati raccolti o trattati;
- esercitare il **diritto alla limitazione** del trattamento ex art. 18 Reg. UE 16/679 in circostanze specifiche;
- esercitare il **diritto alla portabilità** dei dati ex art. 20 Reg. UE 16/679, ovvero richiedere che i dati personali siano trasferiti a terzi in un formato strutturato, standard e leggibile da un dispositivo automatico;
- esercitare il **diritto di opposizione** al trattamento di dati personali che lo riguardano ex art. 21 Reg. UE 16/679, impedendo l'ulteriore uso dei propri dati personali, anche a scopo pubblicitario;
- sollevare riserve in merito ai trattamenti giustificati sulla base dei legittimi interessi del Titolare o in base al pubblico interesse;
- richiedere una copia di un accordo secondo il quale i dati personali sono trasferiti al di fuori dell'AEE;
- obiettare a decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione;
- ricevere notifiche di eventuali violazioni dei dati personali che potrebbero generare rischi significativi per i diritti e le libertà dell'Interessato;
- inviare un reclamo al Garante per la protezione di protezione dei dati.

5. RUOLI E RESPONSABILITÀ

Al fine di gestire correttamente i processi di protezione dei dati personali e delle informazioni trattate sono state individuate e nominate le figure chiave per il trattamento di dati personali citati. In particolare, il Regolamento di cui al [Rif.1] individua specifici ruoli e responsabilità, di cui si riportano di seguito i principali:

1. **Titolare del trattamento** - ha il compito di:
   - nominare, ove necessario, un Data Protection Officer;
   - determinare le finalità e i mezzi del trattamento di dati personali;
   - attuare le misure tecniche e organizzative per garantire la protezione dei dati fin dalla progettazione e per impostazione predefinita;

- accertare che le misure tecniche e organizzative individuate siano adeguate a garantire l'integrità e la riservatezza dei dati personali trattati ex art. 32 Reg. UE 16/679;
- adempiere all'onere di accountability, ovvero essere in grado di dimostrare che le operazioni di trattamento avvengano conformemente ai principi previsti dal GDPR;
- riesaminare e aggiornare, qualora necessario, le misure tecniche e organizzative adottate nonché il Sistema delle Procedure Privacy ivi compresa la presente General Data Privacy Policy;
- nominare, attraverso un atto giuridico, i Designati *interni* ed i Responsabili del trattamento individuando precipuamente quanto previsto dall'art. 28 Reg. UE 16/679;
- nominare gli Autorizzati al trattamento con lettera ad hoc in cui siano indicate le operazioni di trattamento che i medesimi possono compiere sui dati personali e le relative istruzioni operative;
- redigere Informative chiare, complete ed intelligibili a favore degli Interessati;
- acquisire il consenso al trattamento dei dati ex art. 7 Reg. UE 16/679 in maniera chiara, specifica ed inequivocabile;
- predisporre e mantenere aggiornato un Registro dei Trattamenti ex art. 30 Reg. UE 16/679;
- predisporre e mantenere aggiornato un Registro delle Violazioni;
- predisporre, ove necessario, e aggiornare la Valutazione di Impatto ex art. 35 Reg. UE 16/679;
- garantire un agevole esercizio dei diritti previsti in favore degli Interessati ex artt. 15, 16, 17, 18, 20, 21 Reg. UE 16/679;
- attenersi in caso di violazioni dei dati agli obblighi comunicativi previsti dagli artt. 33 e 34 Reg. UE 16/679;
- formare regolarmente il personale sul GDPR, sulla presente General Data Privacy Policy e sui temi legati alla protezione dei dati.

2. **Designato interno al trattamento** è colui che opera nel Management direttivo limitatamente ai poteri e alle deleghe formalmente attribuiti e secondo le aree di specifica competenza. Il Titolare del trattamento delega al Designato interno, tramite formale nomina, specifici poteri in tema privacy nonché particolari funzioni in relazione alle operazioni di trattamento di dati personali.

   In particolare, tale funzione ha il compito di:
   - effettuare operazioni di trattamento sulla base delle istruzioni impartite dal Titolare del trattamento;
   - vigilare sulle operazioni di trattamento compiute da parte dei soggetti autorizzati appartenenti alla propria struttura o al proprio ufficio;
   - effettuare periodiche attività di verifica in merito al mantenimento delle misure di sicurezza con riferimento alla propria struttura o al proprio ufficio.

3. **Autorizzato al trattamento -** ha il compito di:

- effettuare operazioni di trattamento adottando le disposizioni ed istruzioni impartite dal Titolare o dal Designato nominato dal Titolare;
- supportare il Titolare o il Designato nominato dal Titolare per il mantenimento dei più alti livelli di conformità a normative vigenti:
  - comunicando eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
  - segnalando ogni situazione sospetta di anomalia, di potenziale illecito o di evidente violazione di dati personali;
- prestare la più ampia e completa collaborazione al Titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- prestare la più ampia collaborazione al Designato interno al trattamento per garantire un elevato livello di sicurezza e integrità dei dati personali.

4. **Responsabile della protezione dei dati (Data Protection Officer – DPO) -** ha il compito di:
   - informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento, e gli autorizzati al trattamento in merito agli obblighi derivanti dal Regolamento di cui al [Rif. 1] o da altra disposizione nazionale e/o comunitaria;
   - sorvegliare l'osservanza del Regolamento di cui al [Rif. 1];
   - cooperare e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento (i.e. Garante per la protezione dei dati personali).
5. **Responsabile del trattamento ex art. 28 Reg. UE 16/679 -** ha il compito di:
   - trattare dati personali per conto del Titolare del trattamento;
   - seguire le istruzioni fornite dal Titolare del trattamento all'interno dell'Atto di nomina ex art. 28 Reg. UE 16/679;
   - adempiere a tutti gli obblighi, sia documentali che riferiti all'adozione misure tecnico-organizzative idonee e adeguate (ex art. 32 Reg. UE 16/679), previsti dal GDPR;
   - nominare formalmente le persone autorizzate al trattamento dei dati personali (c.d. Incaricati) garantendo che si impegnino alla riservatezza;
   - supportare il Titolare del trattamento per l'adozione delle più ampie misure di sicurezza a protezione dei dati personali trattati;
   - supportare il Titolare del trattamento in caso di esercizio dei diritti da parte degli Interessati;
   - supportare il Titolare del trattamento per la gestione di scenari di Data Breach;
   - cooperare e/o fornire supporto, ove richiesto dal Titolare del trattamento, nell'esecuzione delle attività di analisi dei rischi privacy *"DPIA"* per uno specifico trattamento;
   - comunicare al Titolare qualunque circostanza possa sollevare incertezze in merito al mantenimento dei requisiti di legge previsti dal GDPR;

- qualora necessario, avvalersi di un sub-Responsabile esterno solo previo accordo con il Titolare del trattamento;
- comunicare senza ritardo al Titolare il verificarsi di un Data Breach riguardante i dati personali trattati per suo conto;
- procedere alla cancellazione e alla restituzione dei dati forniti dal Titolare del trattamento, cancellando ogni copia di tali dati, al termine della prestazione fornita e su richiesta del Titolare stesso;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dall'art. 28 Reg. UE 16/679 contribuendo alle attività di ispezione e revisione realizzate dal Titolare stesso o da un altro soggetto da questi incaricato.

6. CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Il Consenso costituisce una delle basi giuridiche che consente un lecito trattamento dei dati personali. Per essere regolarmente conferito e raccolto deve essere *"espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano".*

Tuttavia, il consenso non deve essere considerato l'unica base giuridica per il trattamento dei dati personali dato che, oltre ad essere di difficile raccolta, può essere sempre oggetto di espressa revoca.

Il Consenso dovrà essere richiesto unicamente in quelle circostanze in cui risulti strettamente necessario per le finalità che il Titolare del trattamento intende perseguire con la raccolta dei dati personali (ad es. quando vengono raccolti dati personali per finalità di marketing dietro il consenso del diretto Interessato). Se è necessario il consenso del soggetto, esso deve essere conferito validamente ai sensi della normativa GDPR.

Per *"consenso valido"* si intende ove si verificano le seguenti circostanze:

- *il Consenso deve essere rilasciato liberamente, deve essere specifico e fornire indicazioni non ambigue riguardo il volere del soggetto. Ne consegue che il linguaggio utilizzato per ottenere il consenso dell'interessato per determinate finalità di trattamento deve essere chiaro e idoneo a informare l'individuo riguardo le ragioni per cui il Titolare vuole i dati e come essi saranno utilizzati. Inoltre, il soggetto deve avere la possibilità di scegliere liberamente se accettare o meno. Il consenso deve presentare opzioni separate e distinte ('granulari') nel caso in cui le finalità e le modalità di trattamento dei dati siano molteplici;*
- *il Consenso deve essere rilasciato tramite un'affermazione o un'azione positiva (es. contrassegnare una casella con un segno di spunta o cliccare su un pulsante). Il silenzio, le caselle pre-contrassegnate o l'inattività non sono da considerarsi sufficienti;*
- *il soggetto deve essere informato in merito alla possibilità di revocare il consenso in qualsiasi momento e all'obbligo, per l'impresa, di rispettare tale revoca.*

Il Consenso deve essere nuovamente richiesto in caso di trattamenti di dati personali per una finalità diversa rispetto a quella per cui era stato primariamente raccolto e per la quale rappresenti l'unica base giuridica atta a garantire un trattamento lecito di dati personali.

A meno che non vi siano presupposti giuridici diversi per il trattamento come individuati dall'art. 6 Reg. UE 16/679 e dell'art. 9 Reg. UE 16/679, il consenso esplicito (ossia il consenso che richiede un'affermazione chiara e specifica, oltre a un'azione positiva) è richiesto per il trattamento di dati personali sensibili (ex. art. 9 e 10 Reg. UE 16/679), per processi decisionali automatizzati (compresa l'attività di profilazione ex art. 22 Reg. UE 16/679) e per trasferimenti di dati all'estero. Laddove sia necessario fornire il consenso esplicito, è necessario produrre un'Informativa chiara, completa, concisa e intellegibile da sottoporre al soggetto interessato onde acquisirne il relativo consenso esplicito.

È necessario tenere traccia del consenso conferito (annotando anche come e quando il consenso è stato ottenuto dal soggetto e a cosa egli abbia prestato il proprio consenso) al fine di poter dimostrare la conformità con i requisiti della normativa GDPR.

7. SICUREZZA NELLE OPERAZIONI DI TRATTAMENTO E VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

L'Università è tenuta a valutare quali tipo di misure tecnico-organizzative devono essere implementate al fine di garantire un adeguato livello di sicurezza durante le operazioni di trattamento di dati personali.

Nell'effettuare tale valutazione, l'Università deve prendere in considerazione quanto segue:

- lo stato dell'arte in materia;
- i costi di implementazione;
- la natura, l'oggetto, il contesto e le finalità del trattamento;
- i rischi, nonché la probabilità e gravità delle conseguenze per i diritti e le libertà degli individui generate da tale trattamento.

Nel compiere tale valutazione l'Università dovrà tenere conto dei rischi che derivano in particolar modo dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati e comunque trattati.

Al fine di garantire un livello di sicurezza adeguato, quindi, l'Università dovrà dotarsi di misure che garantiscano l'integrità e la riservatezza dei dati personali trattati, tra cui:

- le pseudonimizzazione e la cifratura dei dati personali;
- l'utilizzo di sistemi atti a garantire su base permanente l'integrità e la riservatezza dei dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;

- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche organizzative al fine di garantire la sicurezza del trattamento.

L'UTSR è tenuta a condurre una Valutazione di Impatto - Data Privacy Impact Assessment (DPIA) che consiste in uno strumento utilizzato per identificare e ridurre i trattamenti ad alto rischio ed il cui procedimento operativo è disciplinato all'interno dell'allegato 10.3 del MOP "*PP3 - Procedura per la compilazione della DPIA"* cui si rimanda per completezza informativa.

Per *"trattamento ad alto rischio"* s'intende qualsiasi procedura che implichi per l'Interessato un rischio più alto del normale in considerazione delle modalità di trattamento dei dati personali o della natura o portata del trattamento che si vuole svolgere. Tale definizione può comprendere i casi in cui si programmi di iniziare a tracciare/monitorare i soggetti per finalità di marketing o qualora si preveda di trasferire un quantitativo significativo di dati da un sistema a un altro.

Si è tenuti a condurre una DPIA in occasione dell'implementazione di significativi programmi di cambiamento dei sistemi o delle attività che interessano il trattamento dei dati personali.

Ai sensi del Reg. UE 16/679, le operazioni di trattamento per le quali è necessario effettuare una valutazione di impatto sono le seguenti:

- utilizzo di nuove tecnologie (ad esempio nuovi sistemi o processi informatici);
- operazioni di trattamento su larga scala di categorie particolare di dati personali di cui all'art. 9 Reg. UE 16/679, o dati relativi a condanne penali ex art. 10 Reg. UE 16/679;
- valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato, compresa la profilazione, e sulla quale fondano decisioni che producono effetti giuridici o incidono significativamente sui diritti e le libertà delle persone fisiche. Per *"processo decisionale automatizzato",* o Automated Decision Making (ADM), si intende un processo attraverso il quale il trattamento viene eseguito in modo esclusivamente automatizzato (compresa la profilazione), modalità che produce effetti legali o conseguenze significative sugli Interessati.

8. DECLINAZIONE DEI PRINCIPI GENERALI NELLE DIVERSE GESTIONI

I principi generali che devono essere recepiti, adottati e rispettati per la protezione dei dati e delle informazioni trattate, in conformità con il Regolamento di cui al [Rif. 1] sono declinati nelle seguenti diverse gestioni:

1. **Gestione organizzativa della sicurezza delle informazioni:**
   - garantire che, all'interno dell'organizzazione, siano identificate le figure chiave per la gestione e governo dei processi di sicurezza delle informazioni. Per ciascuna figura devono essere assegnate specifiche responsabilità attraverso Atti di nomina ad hoc. Devono altresì essere disegnati e adottati processi organizzativi a garanzia della corretta applicazione della presente Policy.
2. **Gestione dei rischi di sicurezza delle informazioni:**

- garantire che sia definito e documentato un processo che consenta l'adozione di criteri e metodologie per l'analisi, la determinazione e la valutazione dei rischi sulla sicurezza delle informazioni e sul loro trattamento. Particolare attenzione e cura dovrà essere posta nell'esecuzione di attività di *"DPIA"* per la valutazione del livello di rischiosità di un trattamento di dati personali e l'individuazione delle più opportune misure di sicurezza da porre in essere a protezione dei dati.

3. Classificazione e protezione dei dati:

- garantire che sia definito e documentato un processo di classificazione e protezione dei dati che definisca le responsabilità e le modalità di trattamento delle informazioni aziendali archiviate, elaborate o condivise all'interno e all'esterno dell'organizzazione, al fine di garantirne una protezione adeguata durante tutto il loro ciclo di vita;
- assicurare che le misure di sicurezza da adottare per la protezione delle informazioni siano valutate in funzione, a titolo esemplificativo ma non esaustivo, dei seguenti criteri minimi di:
  - appetibilità, da valutare in funzione della tipologia del dato;
  - potenziale impatto in caso di perdita, distruzione, alterazione o diffusione del dato, da valutare in funzione della criticità del dato stesso.

4. Gestione accessi logici ai sistemi ed alle applicazioni:

- garantire che sia definito e documentato un processo di gestione degli accessi logici alle risorse informatiche aziendali in grado di restringere gli accessi a tali risorse al solo personale autorizzato;
- garantire che i privilegi di accesso ai sistemi ed alle applicazioni consentano di rispettare i principi di *Need to Know*, *LeastPrivilege*, Privacy by default e Segregation of Duties. Particolare attenzione e cura dovrà essere posta nell'affidamento dei privilegi di accesso *"amministrativi"* per consentire al personale preposto di gestire e governare i sistemi aziendali secondo i regolamenti interni aziendali ed in conformità con il provvedimento di cui al [Rif. 2]. Le utenze di accesso devono essere di tipologia *"nominale"* e solo per specifiche necessità sarà consentito l'uso di utenze di tipologia *"non nominale"* o *"di servizio":* in questi casi verrà assegnato ad ogni utenza uno specifico responsabile che risponderà circa l'utilizzo delle stesse;
- effettuare e documentare periodiche attività di revisione delle utenze presenti sui sistemi e sulle applicazioni, volte alla bonifica delle utenze attive ma inutilizzate, inattive o non conformi ai processi di gestione adottati dall'Università;
- assicurare che sia definito un processo di gestione degli accessi ai siti web, ai social network o simili (ad es. siti commerciali, pagine web personali, blog, spazi personali forniti dagli Internet provider) affinché l'eventuale pubblicazione di contenuti aziendali su un sito Internet, mediante dispositivo di proprietà del Titolare e previo accordo con quest'ultimo, avvenga nel rispetto delle politiche e delle procedure predisposte dall'UTSR. In particolare, il soggetto Autorizzato dovrà sempre rispettare le seguenti direttive:

- assicurarsi che le informazioni pubblicate non abbiano carattere riservato;
- accertarsi che le stesse siano di dominio pubblico e, in tal caso, siano sempre aggiornate, accurate, pertinenti, adeguate e siano mantenute tali;
- non pubblicare foto o immagini di persone specifiche, di altri dipendenti e/o studenti senza aver ottenuto la loro autorizzazione e/o il loro consenso esplicito;
- in caso di richiesta di rimozione da parte dell'Interessato di foto o immagine che lo riguarda, ottemperare a tale richiesta;
- disporre dei permessi adeguati al materiale pubblicato in caso sia soggetto a copyright;
- non utilizzare il sito o il social network per pubblicare contenuti che altri potrebbero trovare offensivi e per esprimere commenti negativi sull'UTSR o sul personale della medesima o per mostrare immagini o foto che potrebbero screditare l'Università.

5. **Gestione della sicurezza fisica ed ambientale:**
   - definire perimetri di sicurezza per proteggere le aree che contengono informazioni e dati personali riservati;
   - definire opportune misure tecniche ed organizzative di sicurezza fisica ed ambientale atte alla protezione dei locali aziendali e dei dati ivi contenuti da minacce naturali, malfunzionamenti di sistemi ed impianti nonché abusi. Particolare attenzione e cura dovrà essere posta nella valutazione delle misure di sicurezza da implementare per la protezione dei locali tecnici e dei data center contenenti impianti di elaborazione;
   - definire opportune misure tecniche ed organizzative per garantire che l'accesso ai locali aziendali, siano essi uffici, depositi, data center, sale tecniche o qualunque altra tipologia di locale, sia limitato al solo personale interno autorizzato. L'accesso del personale esterno, come fornitori, terze parti, outsourcers e visitatori esterni, può avvenire in ragione di uno specifico contratto con la società esterna o il professionista. Le visite del personale esterno devono essere tracciate e monitorate ed il fornitore deve essere identificato con idonei supporti che devono essere esposti e ben visibili.

6. **Gestione degli incidenti ed eventi critici:**
   - mettere in atto misure tecniche ed organizzative volte ad assicurare che i guasti, le anomalie e gli incidenti di sicurezza delle informazioni siano correttamente riconosciuti e gestiti;
   - adottare efficaci sistemi e processi di prevenzione, comunicazione e risposta, al fine di consentire all'organizzazione di adempiere ad eventuali obblighi normativi (i.e. notifica al Garante di Data Breach, per gli incidenti relativi a dati personali) e allo scopo di minimizzare eventuali impatti sul business;
   - tenere in considerazione quanto contenuto nell'allegato n. 10 del MOP *"Sistema delle Procedure Privacy"*, nello specifico PP2 *"Data Breach Management"*.

7. **Gestione della continuità operativa aziendale:**
   - Condurre, con cadenza almeno annuale, attività di analisi della continuità del business aziendale finalizzate alla comprensione degli scenari di minaccia verso la continuità

operativa aziendale, valutazione delle priorità del business aziendale ed implementazione di opportune misure a garanzia della continuità operativa;

- mettere in atto misure tecniche ed organizzative in funzione dei requisiti raccolti in fase di analisi della continuità del business e finalizzate ad assicurare la continuità del business aziendale anche al verificarsi di scenari di guasti, malfunzionamenti, eventi disastrosi o crisi. Particolare attenzione e cura dovrà essere posta nella valutazione delle misure di sicurezza da implementare per garantire la continuità dei sistemi informatici di elaborazione.

8. **Gestione della compliance:**
   - garantire che sia definito e documentato un processo di gestione della compliance volto al mantenimento dei livelli di sicurezza necessari per l'adeguamento ai Regolamenti di cui al [Rif. 1] e [Rif. 2] ed ulteriori normative applicabili, regolamenti aziendali interni, standard organizzativi applicabili e standard internazionali adottati;
   - effettuare periodicamente verifiche interne finalizzate al mantenimento della conformità con le normative applicabili documentandone e condividendone l'esito con il personale apicale chiave per la gestione e governo dei processi di compliance. Le eventuali non conformità rilevate saranno gestite con uno specifico piano di intervento che indicherà le tempistiche e le modalità di rimedio individuate.
9. **Gestione della formazione:**
   - garantire che sia definito e documentato un processo di formazione aziendale strutturato rivolto a tutto il personale interno che, a diverso titolo e con diversi incarichi, effettua operazioni di trattamento di dati personali volto alla sensibilizzazione, istruzione, formazione e addestramento sui regolamenti normativi applicabili e sulle politiche e procedure interne dell'organizzazione di sicurezza e protezione dei dati personali.
10. **Gestione del rapporto con gli Interessati:**
    - garantire che sia definito e documentato un processo di gestione dell'esercizio dei diritti da parte degli Interessati come previsti dagli artt. 15, 16, 17, 18, 20, 21 del Reg. UE 16/679;
    - garantire che sia fornito un adeguato e completo riscontro alle istanze formulate dagli Interessati entro un termine temporale ragionevole;
    - tenere in considerazione quanto contenuto nell'allegato n. 10 *"Sistema delle Procedure Privacy"*, nello specifico PP5 *"Gestione delle istanze degli Interessati"*.
11. **Gestione della crittografia:**
    - garantire che sia definito e documentato un processo di gestione delle soluzioni crittografiche per la gestione degli scenari nei quali le informazioni, per un requisito normativo, di business o per scelta aziendale, necessitano di essere crittografate;
    - garantire che le informazioni critiche, oggetto di specifici requisiti normativi (i.e. i dati personali, particolari e giudiziari) o connesse a proprietà intellettuali dell'Università, archiviate, trasmesse o pubblicate su canali di comunicazione insicura, come la rete internet, siano oggetto di cifratura. Particolare attenzione e cura dovrà essere posta per i

processi di trasmissione di tali informazioni al di fuori della rete aziendale, attraverso lo strumento di produttività della posta elettronica, in particolare devono essere sempre adottati i seguenti accorgimenti:

- il contenuto informativo critico della trasmissione deve essere criptato;
- lo scambio della chiave di decifratura, qualora si utilizzino tecniche di cifratura simmetrica, deve avvenire attraverso un canale separato dal canale di trasmissione;
- la trasmissione deve essere circoscritta ai soli destinatari titolati alla ricezione di tali informazioni;

- redigere e divulgare opportune istruzioni sulle modalità di utilizzo degli strumenti crittografici aziendali al fine di rendere edotto tutto il personale e minimizzare potenziali utilizzi impropri dei suddetti strumenti ed i connessi rischi di sicurezza.

12. Gestione delle terze parti:

- garantire che sia definito e documentato un processo di gestione delle terze parti atto alla definizione dei requisiti di sicurezza delle informazioni volti a mitigare i rischi associati all'accesso agli asset aziendali da parte dei fornitori, terze parti, outsourcers e visitatori esterni;
- assicurare che i contratti con i fornitori contengano opportuni requisiti di sicurezza per i processi di elaborazione, archiviazione e trasmissione volti alla tutela del patrimonio informativo dell'Università;
- assicurare che venga predisposta un'adeguata nomina a Responsabile al trattamento dei dati personali che rifletta integralmente i contenuti dell'art. 28 Reg. UE 16/679 (si rinvia all'allegato n. 4 del MOP, nello specifico all'Atto di nomina del Responsabile al trattamento ex art. 28 Reg. UE 16/679);
- effettuare verifiche periodiche sulle forniture volte a monitorare la conformità dell'erogazione dei servizi concordati.

13. Gestione dello sviluppo ed acquisizione dei sistemi informativi:

- garantire che sia definito e documentato un processo di gestione dello sviluppo ed acquisizione dei sistemi informativi mirato a garantire che siano presenti ed implementati, sin dalla progettazione o acquisizione di un nuovo sistema informativo, specifici principi di sicurezza delle informazioni volti alla protezione dei dati, in accordo con il principio Privacy by design;
- definire specifici processi per il controllo ed il tracciamento dei cambiamenti/aggiornamenti ai sistemi informativi, mirati a garantire che le modifiche siano correttamente testate in ambienti distinti dall'ambiente di operatività reale o *"di produzione"*, approvate dal personale chiave responsabile della gestione dei sistemi informativi e documentate, prima della loro applicazione;
- in caso di aggiornamento dei sistemi informativi, o di loro variazione, garantire che vengano aggiornate la Valutazione di impatto e le misure di sicurezza qualora con tale

sistema siano differenti rispetto alle precedenti, nonché i contenuti del Registro dei trattamenti.

14. **Gestione delle vulnerabilità:**
    - garantire che sia definito e documentato un processo di gestione delle vulnerabilità volto alla rilevazione, valutazione e gestione delle vulnerabilità di sicurezza e di eventuali malware che affliggono i sistemi e le applicazioni;
    - garantire che il processo di rilevazione delle vulnerabilità sia eseguito con cadenza periodica, mediante l'esecuzione di specifiche attività meglio note come *"Vulnerability Assessment"* documentandone gli esiti. Tale processo dovrà essere in ogni caso attivato a fronte di eventuali cambiamenti dei sistemi informativi o delle applicazioni ed all'acquisizione o sviluppo di nuovi sistemi;
    - garantire che i sistemi e le applicazioni siano sempre aggiornati con i più recenti aggiornamenti di sicurezza rilasciati dai fornitori di servizi informatici (i.e. *"Vendor"*) in modo da garantire i più elevati livelli di protezione contro le minacce informatiche.

15. **Gestione delle risorse tecnologiche aziendali:**
    - garantire che sia definito e documentato un processo di gestione delle risorse tecnologiche aziendali, in grado di creare e manutenere costantemente un inventario di tali risorse volto al mantenimento dei più elevati livelli di sicurezza fisica e logica a protezione di tali asset.

16. **Gestione e monitoraggio della rete:**
    - mettere in atto misure tecniche ed organizzative volte ad assicurare un adeguato funzionamento dei sistemi e degli apparati di rete ed un continuo controllo su tutte le componenti dei sistemi;
    - garantire il monitoraggio dello stato della rete per garantire che, a fronte di eventuali malfunzionamenti dei sistemi che possono rallentare o bloccare l'operatività aziendale, sia attivato un intervento tempestivo;
    - effettuazione di periodici Risk Assesment e Penetration Test al fine di valutare la sicurezza della rete informatica e la tenuta delle misure di sicurezza implementate.

17. **Gestione della sicurezza della rete e delle infrastrutture:**
    - garantire che sia definito e documentato un processo di gestione di sicurezza della rete e delle infrastrutture volto al mantenimento dei più elevati livelli di sicurezza e che garantisca i più elevati livelli di continuità operativa, in accordo con il principio Defense in depth;
    - garantire che i servizi infrastrutturali siano stati oggetto di attività di *hardening*, mirate al restringimento dei soli servizi necessari e alla modifica delle impostazioni di *"default"*, sia a livello di settaggi di sicurezza che di utenze per l'accesso logico;
    - applicare le best practices di sicurezza per la segmentazione delle reti aziendali interne, in modo da realizzare *"zone"* di sicurezza con diversi livelli di protezione;
    - garantire che i servizi esposti su rete pubblica e sulle reti aziendali interne siano adeguatamente protetti da strumenti di rilevazione e protezione contro attacchi informatici.

9. DIRECT MARKETING

Per le attività di direct marketing elettronico (ad esempio tramite e-mail, sms o chiamate automatizzate) è necessario il consenso dell'Interessato.

Il diritto di opposizione al direct marketing deve essere esplicitamente offerto all'Interessato in modo chiaro affinché sia chiaramente distinguibile da altre informazioni.

Qualora un soggetto manifesti la volontà di non ricevere pubblicità di direct marketing, la richiesta deve essere accolta tempestivamente eliminando i suoi dati il prima possibile.

10. CONDIVISIONE DEI DATI PERSONALI

È possibile condividere i dati personali con soggetti terzi, come i fornitori di servizi, unicamente quando:

- siano stati individuati come destinatari o Responsabili esterni del trattamento conformemente a quanto indicato nell'Informativa sulla privacy fornita all'Interessato e, se necessario, è stato ottenuto il suo consenso;
- è stata sottoscritta una apposita nomina ex art. 28 Reg. UE 16/679 con i Responsabili esterni;
- i Responsabili esterni hanno accettato di rispettare i relativi standard, policy e procedure di sicurezza sui dati ed hanno implementato adeguate misure di sicurezza;
- il trasferimento è conforme ad eventuali limitazioni di trasferimento transfrontaliero.

Nei rapporti con i Responsabili del trattamento, occorre preliminarmente eseguire un processo di valutazione necessario a comprendere:

- che tratteranno i dati personali in conformità alle leggi vigenti;
- la finalità per la quale utilizzeranno tali dati;
- chi ne avrà accesso;
- dove saranno archiviati/trasferiti;
- le misure di sicurezza tecniche e organizzative

tramite l'ausilio dell'allegato 1 all'Atto di nomina a Responsabile al trattamento ex art. 28 Reg. UE 16/679 cui si rimanda.

In caso di esito positivo della valutazione globale, è necessario sottoscrivere, a latere del contratto di servizio con il medesimo stipulato al cui interno dovranno essere inserite delle specifiche clausole predisposte ad hoc, una apposita nomina privacy a Responsabile del trattamento che rifletta in toto i contenuti dell'art. 28 Reg. UE 16/679.

Una volta concluso il rapporto di collaborazione con il Responsabile esterno, occorre assicurarsi, in modo tracciato tramite una specifica conferma scritta, che quest'ultimo cancelli in modo sicuro e permanente i dati personali conservati a nome dell'Università affinché non possano più accedervi in futuro.

11. VIOLAZIONE DEI DATI PERSONALI

In accordo con quanto sancito nel GDPR, l'Università è tenuta alla comunicazione di eventuali violazioni dei dati personali all'Autorità competente e, in alcuni casi, all'Interessato stesso. Tale denuncia dovrà essere notificata secondo tempistiche e modalità precise come previste dagli artt. 33 e 34 Reg. UE 16/679.

Per *"violazione dei dati personali"* si intende qualsiasi atto o omissione che comprometta la sicurezza, riservatezza, integrità o disponibilità dei dati personali o i sistemi protettivi fisici, tecnici, amministrativi o organizzativi implementati dall'Università stessa o dai propri fornitori di servizi esterni. Ciò include:

- la distruzione dei dati personali, accidentale o dolosa;
- una modifica dei dati personali non autorizzata, accidentale o dolosa;
- una perdita di dati personali, accidentale o dolosa;
- un accesso ai dati personali non autorizzato, accidentale o doloso;
- una divulgazione non autorizzata, accidentale o dolosa.

Per completezza informativa si rimanda ai contenuti dell'allegato n. 10 del MOP, nello specifico alla PP2 *"Data Breach Management"*.

12. SISTEMA SANZIONATORIO PRIVACY PREVISTO DAL GDPR

Le sanzioni applicabili in caso di violazione, individuate nel Regolamento, sono pari a:

1. fino ad euro 10.000.000,00, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a:
   - minori,
   - obblighi del Titolare e Responsabile ex art. 28 Reg. UE 16/679,
   - obblighi dell'organismo di certificazione,
   - obblighi dell'organismo di controllo,
2. fino ad euro 20.000.000,00, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a:
   - principi di base del trattamento, comprese le condizioni relative al consenso,
   - i diritti degli Interessati,
   - il trasferimento dati a paesi extra UE,
   - gli obblighi imposti dagli stati membri per specifiche categorie,
   - l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

Aspetto essenziale per l'effettività e l'idoneità del Modello Organizzativo Privacy è costituito dalla predisposizione di un adeguato *"Sistema disciplinare Privacy"* per la violazione delle regole di condotta imposte ai fini della prevenzione delle violazioni e, in generale, delle Procedure Privacy interne previste dal MOP.

Per completezza informativa si rimanda ai contenuti dell'allegato 2 del MOP *"Sistema disciplinare Privacy"*.

13. SISTEMA DOCUMENTALE PRIVACY

Il GDPR richiede il mantenimento di documenti completi, corretti e aggiornati afferenti tutte le attività di trattamento dei dati eseguite.

Per tale motivo si richiama l'attenzione dei destinatari della presente General Data Privacy Policy sull'importanza di mantenere uno strutturato, organico e puntuale archivio della documentazione della quale si compone il Modello Organizzativo Privacy dell'Università.

Il presente documento è diffuso all'interno di Università Telematica San Raffaele Roma S.r.l. ed è comunicato ai destinatari del MOP che hanno l'obbligo di:

- conformarsi alle prescrizioni messe a punto dall'Università;
- astenersi dall'attuare comportamenti che possano, anche in modo potenziale o involontario, integrare una violazione nella gestione e nel trattamento dei dati.

La Direzione s'impegna a riesaminare periodicamente la **General Data Privacy Policy** affinché la gestione aziendale possa tendere ad un progressivo miglioramento delle prestazioni attuando le misure correttive ritenute necessarie.

Ogni modifica ai principi del presente documento è soggetta all'approvazione del Consiglio di Amministrazione.