REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sommario

1. AMBITO DI APPLICAZIONE

1. Il presente regolamento disciplina il trattamento di dati personali effettuato dall'Università degli Studi Roma Tre in applicazione dei principi di cui al Regolamento (UE) 679/2016 ("GDPR") e al Decreto Legislativo 30 giugno 2003 n. 196, come successivamente modificato ("Codice Privacy").
2. L'Università provvede al trattamento dei dati personali per lo svolgimento dei propri fini istituzionali, nei limiti stabiliti dallo Statuto, dalle leggi e dai regolamenti vigenti e in ogni caso nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con riferimento particolare alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
3. L'Università considera il trattamento lecito, corretto e trasparente dei dati personali una azione prioritaria al fine di instaurare e mantenere un rapporto di fiducia con gli studenti e le studentesse, il personale e i terzi interessati.

2. DEFINIZIONI

Ai fini del presente Regolamento si intende per:

1. "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2. "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3. "dati particolari" o "dati sensibili": dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
4. "titolare del trattamento" o "data controller": 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;
5. "responsabile del trattamento" o "data processor": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
6. "responsabile della protezione dei dati" o "data protection officer" o "DPO": la persona incaricata dall'Università ai sensi dell'art. 37 del GDPR.
7. "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;

8. "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;
9. "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;
10. "destinatario dei dati": 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;
11. "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;
12. "consenso dell'interessato" o "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, che i dati personali che lo riguardano siano oggetto di trattamento;
13. "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;
14. "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;
15. "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;
16. "dati giudiziari": dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
17. “incaricati” le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile”;
18. “comunicazione” il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione";
19. "diffusione” il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione";
20. “dato anonimo” il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
21. “banca di dati” qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti”;
22. “strumenti elettronici” gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento”;

23. “autenticazione informatica” l’insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell’identità”;
24. “credenziali di autenticazione” i dati ed i dispositivi in possesso di una persona da questa conosciuti o ad essa univocamente correlati, utilizzati per l’autenticazione formale”;
25. “parola chiave” componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

3. PRINCIPI GENERALI

1. Il trattamento dei dati personali da parte dell'Università segue i principi del GDPR e del Codice Privacy.
2. In particolare, i dati sono trattati tenendo conto dei seguenti principi:
    a. Principio di liceità, correttezza e trasparenza: i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
    b. Principio di limitazione della finalità: i dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità. Conformemente all'articolo 89, paragrafo 1 del GDPR, un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è considerato compatibile con le finalità iniziali.
    c. Principio di minimizzazione del dato: i dati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
    d. Principio di esattezza: i dati sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
    e. Principio di limitazione della conservazione: i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente alle disposizioni specifiche del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.
    f. Principio di integrità e riservatezza: i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.
3. Inoltre, in conformità alla normativa vigente, l’Università non richiederà il consenso dell’interessato in tutti i casi in cui è individuabile in modo certo un interesse pubblico rilevante o un'altra idonea base giuridica differente dal consenso. Le modalità di individuazione della base giuridica del trattamento sono indicate nell’*Allegato 5 - Istruzioni per il corretto trattamento dei dati personali*.

4. CIRCOLAZIONE DEI DATI ALL’INTERNO DELL’UNIVERSITÀ

1. L'accesso ai dati personali da parte delle strutture amministrative, di servizio, didattiche e scientifiche e dei dipendenti dell'Università volto al perseguimento dei fini istituzionali è ispirato al principio della libera circolazione delle informazioni all’interno dell’Ateneo, secondo il quale

l'Università provvede all'organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione.

2. Ogni richiesta d'accesso ai dati personali da parte delle strutture e dei dipendenti dell'Università, debitamente motivata e connessa con lo svolgimento dell'attività inerente alla loro specifica funzione, sarà soddisfatta in via diretta e senza ulteriori formalità nella misura necessaria, pertinente e non eccedente, al perseguimento dell'interesse istituzionale e delle finalità del trattamento. Laddove invece la richiesta fosse finalizzata a un utilizzo ulteriore rispetto alle finalità per le quali il dato è stato raccolto, sarà necessario effettuare una valutazione specifica come indicato nel successivo art. 11.

5. TITOLARE DEL TRATTAMENTO

1. L'Università degli Studi Roma Tre è titolare del trattamento relativamente a tutti i dati personali detenuti dall'Università, raccolti o meno in banche dati, automatizzate o cartacee, salvo il caso in cui l'Università sia stata designata quale responsabile del trattamento mediante apposito atto giuridico vincolante.
2. Il titolare del trattamento è raggiungibile all'indirizzo e-mail privacy@uniroma3.it e PEC privacy@ateneo.uniroma3.it.

6. CONTITOLARE

1. Quando uno o più titolari del trattamento determinano congiuntamente con l'Università le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.
2. L'Università e il Contitolare del trattamento determinano in modo trasparente, mediante un accordo interno, i rispettivi obblighi in merito all'osservanza del Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni richieste dall'Informativa privacy, salvo quanto previsto dall'art. 26 del GDPR.
3. L' accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
4. L'interessato può esercitare i propri diritti nei confronti di ciascun contitolare del trattamento.

7. RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

1. Il Rettore designa, con apposito decreto, il soggetto responsabile della protezione dei dati (DPO) in conformità alle disposizioni del GDPR.
2. Il DPO designato è tenuto a:
    a. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla disciplina in materia di protezione dei dati personali;
    b. sorvegliare l'osservanza della disciplina in materia di protezione dei dati personali nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
    c. fornire il parere in merito alla valutazione d'impatto sulla protezione dei dati, in conformità al modello di cui all'*Allegato 10 - Valutazione di impatto*, ai sensi dell'articolo 35 del GDPR e alla normativa di attuazione emanata dal Garante per la protezione dei dati personali;

   d. cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto con detta autorità di controllo per ogni questione connessa ai trattamenti posti in essere dall'Università, ivi inclusa la consultazione preventiva di cui all'articolo 36 del GDPR;
   e. coordinare la procedura di cui all'*Allegato 6 - Procedura di notifica delle violazioni* nel caso si verifichi una violazione dei dati.
3. Al fine di garantire la piena autonomia del DPO nell'esercizio delle sue funzioni, l'Università assicura che il DPO:
   a. sia dotato delle risorse necessarie per l'espletamento dei suoi compiti;
   b. possa accedere ad ogni informazione o dato ritenuto necessario per lo svolgimento delle proprie funzioni;
   c. possa avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture dell'Università e di consulenti esterni.
4. Il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni rilevanti riguardanti la protezione dei dati personali. A tal fine, il DPO:
   a. è informato preventivamente ogniqualvolta debbano essere assunte decisioni, a tutti i livelli, che impattino sulla protezione dei dati;
   b. è tempestivamente informato dell'esistenza, o della possibilità che si verifichino, violazioni dei dati o altro incidente.
5. Il DPO invia al Rettore e al Direttore Generale una relazione annuale sullo stato di implementazione dei processi volti a garantire il rispetto della normativa in materia di protezione dei dati personali all'interno dell'Università, sulle attività compiuta nel periodo di riferimento e sulle linee generali di intervento per il periodo successivo.
6. Il responsabile per la protezione dei dati di Ateneo è raggiungibile all'indirizzo e-mail rpd@uniroma3.it e PEC rpd@ateneo.uniroma3.it.

8. RESPONSABILE DEL TRATTAMENTO

1. Il responsabile del trattamento è la persona fisica o giuridica, o altro organismo che tratta dati personali per conto del titolare del trattamento. Sono pertanto da considerarsi responsabili del trattamento i fornitori selezionati dall'Università per l'erogazione di servizi che trattano dati personali.
2. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
3. Il contratto o altro atto giuridico è sottoscritto dal titolare del trattamento o dal Direttore Generale o dal Dirigente dell'Area Contratti o da altra persona delegata dal titolare del trattamento. Un fac-simile di contratto è riportato nell'*Allegato 8 - Nomina Responsabile Trattamento*.

9. RESPONSABILE INTERNO DEL TRATTAMENTO

1. All'interno della propria organizzazione l'Università individua dei soggetti responsabili (definiti, singolarmente, "responsabile interno del trattamento") che nei limiti di poteri gerarchici e funzionali adeguati alla natura della posizione ricoperta:
   a. coadiuvano il titolare nella definizione delle finalità e delle modalità di trattamento;

b. collaborano con il titolare nell'individuare i mezzi atti a garantire l'osservanza della normativa sulla protezione dei dati personali;
c. sovrintendono alle attività di trattamento dei dati;
d. garantiscono il rispetto della normativa di riferimento e del presente regolamento;
e. controllano la corretta esecuzione da parte degli incaricati delle istruzioni per il trattamento dei dati personali.

2. I responsabili interni del trattamento sono individuati come segue:

CONTESTO	RESPONSABILE INTERNO DEL TRATTAMENTO
Segreteria del Rettore/Direzione Generale	Responsabile al vertice della segreteria
Singolo Ufficio dell'Amministrazione Centrale	Responsabile al vertice dell'Ufficio
Dipartimenti	Segretario Amministrativo, per la Didattica e per la Ricerca
Centri	Segretario della struttura
Scuole	Segretario per la Didattica
Sistema Bibliotecario di Ateneo	Responsabile di biblioteca d'area
Insegnamento o altra attività formativa	Docente titolare
Progetti di ricerca	Docente responsabile/referente scientifico del progetto

3. Il responsabile interno del trattamento si attiene alle istruzioni impartite dall'Università, o dal diverso titolare del trattamento che ha provveduto a designare l'Università quale responsabile del trattamento, e in particolare si impegna a:
   a. istruire e garantire il rispetto del presente regolamento da parte degli incaricati che svolgono le funzioni all'interno della propria struttura organizzativa;
   b. verificare affinché soltanto gli incaricati che hanno ricevuto adeguate istruzioni accedano alle operazioni di trattamento dei dati;
   c. segnalare tempestivamente carenze delle misure organizzative e tecniche messe in atto per assicurare la protezione dei dati personali;
   d. assicurare che per ogni singolo trattamento posto in essere sia stata individuata una opportuna base giuridica per il trattamento;
   e. assicurare che i contratti con i responsabili del trattamento esterni all'Università (es. fornitori) contengano le disposizioni necessarie, in conformità con quelle previste all'*Allegato 8 - Nomina Responsabile Trattamento*;
   f. per i trattamenti che hanno come base giuridica il consenso, predisporre le misure organizzative atte a garantire la conservazione della copia del consenso acquisito, sia esso cartaceo o elettronico, da parte della struttura autorizzata al trattamento;
   g. assicurare che i nuovi trattamenti effettuati dalla propria struttura organizzativa per conto dell'Università, siano inseriti nel registro delle attività di trattamento. In particolare, il registro delle attività del trattamento riporterà le seguenti informazioni:
      i. le finalità del trattamento;
      ii. la descrizione delle categorie di interessati e delle categorie di dati personali;

iii. se del caso, le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali
iv. se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e le garanzie adottate per tali trasferimenti;
v. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati, in conformità con le tempistiche individuate dai regolamenti dell'Università;
vi. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati.

h. comunicare al titolare, per il tramite del DPO, l'intenzione di avviare qualsivoglia nuovo trattamento che, prevedendo l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà degli interessati, affinché il DPO possa fornire il proprio parere in merito alla valutazione di impatto. Il responsabile interno del trattamento è sempre tenuto ad informare il DPO laddove il trattamento che intende compiere comporti:
    i. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
    ii. il trattamento, su larga scala, di categorie particolari di dati sensibili o di dati giudiziari;
    iii. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
i. fornisce immediato riscontro alle richieste avanzate dagli interessati entro il termine massimo di 30 giorni dalla ricezione, seguendo le istruzioni di cui al paragrafo che segue. Laddove la richiesta avanzata dagli interessati presenti elementi di particolare rilevanza ne dà immediata comunicazione al DPO.

10. INCARICATO DEL TRATTAMENTO

1. È incaricato del trattamento qualsiasi persona fisica legittimata, sulla base del ruolo ricoperto nell'organizzazione, a compiere operazioni di trattamento su dati personali. Pertanto, a far data dall'entrata in vigore del presente regolamento, sono incaricati del trattamento per conto dell'Università, senza che si renda necessaria alcuna ulteriore formalità, i singoli dipendenti, collaboratori, addetti ai servizi, borsisti cui sono state assegnati compiti specifici nell'ambito delle borse di collaborazione di ateneo, ecc..
2. Oltre alle istruzioni di carattere generale il responsabile interno del trattamento può fornire all'incaricato ulteriori indicazioni e istruzioni qualora lo specifico trattamento lo richieda.
3. Sono altresì incaricati del trattamento i soggetti individuati quali responsabili interni del trattamento.
4. Il responsabile interno del trattamento può designare quale incaricato del trattamento un soggetto terzo che debba svolgere operazioni di trattamento di dati personali, ad esclusione dei "dati sensibili", per un periodo limitato di tempo. La designazione avviene in forma scritta e contestualmente sono fornite all'incaricato le istruzioni necessarie a garantire il

corretto trattamento in coerenza con gli obiettivi dell'Università e nel rispetto dei principi generali in materia di protezione dei dati personali.

5. L'incaricato del trattamento si impegna a seguire scrupolosamente le istruzioni fornite in *Allegato 5 - Istruzioni per il corretto trattamento dei dati personali,* si attiene alle istruzioni specifiche fornite dal responsabile interno del trattamento, nonché alle eventuali istruzioni impartite dal diverso titolare del trattamento che ha provveduto a designare l'Università quale responsabile del trattamento.
6. Laddove l'incaricato del trattamento abbia un dubbio circa le operazioni da intraprendere o circa la legittimità del trattamento, deve darne tempestiva comunicazione al responsabile interno del trattamento o, in caso di irraggiungibilità di quest'ultimo, al DPO.

11. ATTIVITÀ DI TRATTAMENTO E OBBLIGHI DI INFORMATIVA

1. Prima di porre in essere qualsiasi attività di trattamento, il responsabile interno del trattamento o il singolo incaricato del trattamento deve accertarsi che il trattamento in questione sia sussumibile sotto uno qualsiasi dei trattamenti previsti nelle seguenti informative:
    a. Informativa per gli studenti e le studentesse;
    b. Informativa per il personale;
    c. Informativa per fornitori ed enti;
    d. Informativa sintetica ed altre informative specifiche.
2. Laddove il trattamento effettuato non sia sussumibile in alcuni dei trattamenti individuati, occorrerà:
    a. richiedere al titolare, per il tramite del DPO, di inserire il trattamento all'interno del registro delle attività di trattamento;
    b. richiedere al titolare, per il tramite del DPO, di modificare la relativa informativa, anche mediante specificazione di un trattamento già ivi indicato, o, in alternativa, sottoporre all'approvazione del titolare, per il tramite del DPO, una informativa ad hoc per il trattamento in questione.
3. Nel caso in cui sussistano dubbi circa la legittimità di un trattamento, occorre informare tempestivamente il responsabile interno del trattamento e il DPO.
4. Nessun ulteriore trattamento rispetto a quelli indicati nel registro delle attività di trattamento può essere avviato senza la preventiva autorizzazione del titolare del trattamento.
5. Nessuna informativa ulteriore a quelle adottate con il presente regolamento può essere utilizzata senza la preventiva autorizzazione.
6. Al fine di rendere omogenee le procedure di raccolta delle informazioni e di garantire i diritti dell'interessato, nell'*Allegato 7 - Clausole standard* sono riportate le clausole contrattuali da inserire nei bandi, contratti, modulistica e ogni qualvolta vengono raccolti dati personali.

12. TRATTAMENTI A FINI DI STUDIO E DI RICERCA

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico l'Università può effettuare trattamenti con finalità di studio e di ricerca. In tali ambiti, l'Università si conforma alle prescrizioni specifiche adottate dal Garante per la protezione dei dati personali, tra cui, ove applicabili, le disposizioni di cui agli artt. 97 e ss. del Codice Privacy, le prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, le prescrizioni relative al

trattamento dei dati genetici nonché le regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica.

13. VALUTAZIONE DI IMPATTO

1. Nei casi previsti dall'art. 35 del GDPR e dalla normativa attuativa in materia, il responsabile interno del trattamento cura la redazione della valutazione di impatto secondo il modello fornito in *Allegato 10 - Valutazione di impatto*. La valutazione di impatto è trasmessa dal Dirigente compente, Direttore di Dipartimento/Centro, Presidente della Scuola al DPO per il relativo parere.
2. Il titolare del trattamento adotta i provvedimenti del caso in merito alla valutazione di impatto, sentito il parere del Direttore Generale, del Dirigente competente a seconda degli uffici interessati e del DPO.

14. VIOLAZIONI DEI DATI

1. Una violazione di dati personali 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. Ciò può derivare da molteplici fattori quali, a titolo esemplificativo, la sottrazione delle chiavi di accesso ad un archivio cartaceo o informatico, lo smarrimento di un personal computer, lo smaltimento di documenti non distrutti. Una violazione dei dati può, se non affrontata in modo adeguato e tempestivo, provocare danni rilevanti agli interessati, quali, ad esempio il furto o l'usurpazione d'identità, pregiudizio alla reputazione, o qualsiasi altro danno economico o sociale significativo. Conseguentemente, la violazione può determinare l'esposizione a rischi gravemente compromettenti per l'Università, ivi inclusi quelli di natura economica. In taluni casi, potrebbe altresì configurare fattispecie di reato.
2. Pertanto, qualora si verifichi una violazione dei dati personali o si sospetti una violazione dei dati personali, gli incaricati del trattamento coinvolti informano tempestivamente il proprio responsabile interno del trattamento e/o il DPO subito dopo essere venuti a conoscenza della violazione, seguendo la procedura descritta nell'*Allegato 6 - Procedura di notifica delle violazioni*.
3. Il DPO provvede a convocare, se necessario, una riunione con gli interlocutori interessati al fine di acquisire maggiori informazioni ed eventualmente decidere le azioni successive.
4. Laddove il DPO o il Titolare ritengano che, anche soltanto all'esito di un maggiore approfondimento, possa ricorrere la necessità di notificare la violazione al Garante per la protezione dei dati personali, è avviata la procedura di cui all'*Allegato 6 - Procedura di notifica delle violazioni*. Nel caso in cui la violazione concerne un trattamento svolto dall'Università in qualità di responsabile del trattamento, l'Università informa il titolare del trattamento senza ingiustificato ritardo.
5. Ogni segnalazione pervenuta all'Università da parte degli incaricati o dei responsabili interni deve essere conservata a documentare l'avvenuta violazione, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

15. TEMPI DI CONSERVAZIONE DEI DATI E CESSAZIONE DEL TRATTAMENTO

1. Uno dei principi fondamentali alla base del corretto trattamento dei dati personali è quello della conservazione. In base a tale principio, i dati personali devono essere conservati in una forma che

consenta l'identificazione degli interessati per un tempo non superiore al conseguimento della finalità per cui sono trattati, fatto salvo il caso di obblighi di legge particolari.

2. Al venire meno di tali finalità o degli obblighi di legge, i dati personali o i documenti che li contengono devono essere distrutti, de-identificati o anonimizzati.
3. I documenti in formato cartaceo o digitale afferenti ad una delle categorie di cui all'*Allegato 9 – Periodo di conservazione dei dati* devono essere conservati in conformità con quanto stabilito nello stesso, salvo che sussista una valida ragione per l'Università per trattenerli, quale la presenza di una controversia giudiziaria, la richiesta da parte di un'autorità competente, o altri motivi specifici che ne giustifichino una conservazione prolungata. In tali casi, la conservazione deve essere autorizzata dal responsabile interno del trattamento, senza necessità di alcuna ulteriore autorizzazione.
4. Ciascun responsabile interno del trattamento è responsabile per l'identificazione dei documenti che devono essere distrutti o conservati e per la determinazione del tempo adeguato di conservazione per quanto di proprio competenza. La distruzione di documenti contenenti dati personali, nonché delle eventuali copie digitali, deve essere operata mediate la triturazione (in caso di supporti fisici) o mediante cancellazione sicura (in caso di supporti elettronici). Documenti diversi da quelli precedenti possono essere distrutti mediante operazioni di riciclo.
5. Limitatamente all'ambito di competenza dei poteri della Soprintendenza Archivistica la documentazione originale non potrà in alcun caso essere distrutta senza la previa autorizzazione della stessa.

16. DIRITTI DELL'INTERESSATO

1. Ogni interessato ha diritto di richiedere all'Università l'esercizio dei diritti previsti dal GDPR. In particolare, si tratta dei diritti di accesso, rettifica, cancellazione nonché del diritto alla portabilità dei dati, del diritto di limitazione del trattamento e del diritto di opposizione al trattamento, ove ne ricorrano i presupposti. Di seguito è fornita una breve esplicazione dei diritti riconosciuti ai soggetti interessati dal trattamento:
    a. il diritto di accesso consente all'interessato di ottenere conferma che sia o meno in corso un trattamento dei suoi dati personali da parte dell'Università e, se del caso, accedere a tali dati e alle informazioni ad essi relative;
    b. il diritto di rettifica consente all'interessato di ottenere la modifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, di ottenere l'integrazione dei dati personali incompleti;
    c. il diritto alla cancellazione consente all'interessato di ottenere la cancellazione dei dati che lo riguardano senza ingiustificato ritardo (ad es. quando i suoi dati personali non sono più necessari in relazione alle finalità per cui sono stati raccolti), fatte salve le eccezioni previste dalla normativa applicabile (es. quando la conservazione dei dati è necessaria per il rispetto di obblighi di legge applicabili all'Università);
    d. il diritto alla portabilità dei dati consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e che egli ha fornito all'Università;
    e. il diritto alla limitazione del trattamento consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di ottenere la limitazione del trattamento dei propri dati personali;
    f. il diritto di opposizione al trattamento consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di opporsi al trattamento dei suoi dati personali. In tali

casi l'Università si asterrà dal trattare ulteriormente i dati personali dell'interessato, salvo che l'Università stesso possa dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Inoltre, in qualsiasi momento, l'interessato ha il diritto di:
    a. revocare il consenso eventualmente prestato, senza con ciò pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
    b. proporre reclamo al Garante per la protezione dei dati personali se ritiene che il trattamento che lo riguarda violi le disposizioni in materia di protezione dei dati personali.

17. ELENCO ALLEGATI

1. Per le disposizioni specifiche si fa riferimento ai seguenti allegati:
    a. Allegato 1 - Informativa per gli studenti e le studentesse
    b. Allegato 2 – Informativa per il personale
    c. Allegato 3 – Informativa per i fornitori ed enti
    d. Allegato 4 – Informativa sintetica ed altre informative specifiche
    e. Allegato 5 - Istruzioni per il corretto trattamento dei dati personali
    f. Allegato 6 - Procedura di notifica delle violazioni
    g. Allegato 7 - Clausole standard
    h. Allegato 8 - Nomina Responsabile Trattamento
    i. Allegato 9 – Periodo di conservazione dei dati
    j. Allegato 10 - Valutazione di impatto

18. DISPOSIZIONI FINALI

1. Per tutto quanto non espressamente disciplinato nel presente Regolamento si applicano le disposizioni del GDPR e tutte le norme vigenti in materia, nonché i Regolamenti d'Ateneo purché non confliggenti.
2. Il presente Regolamento potrà essere aggiornato a seguito dell'esperienza maturata in Ateneo, dell'evoluzione tecnologica e organizzativa, nonché dell'emanazione di normativa in merito alla protezione dei dati personali. L'aggiornamento o la modifica di uno o più allegati al Regolamento non comporta la revisione dell'intero Regolamento.

INFORMATIVA PER GLI STUDENTI E LE STUDENTESSE

Informativa relativa al trattamento dei dati personali relativi alle persone fisiche che accedono alle attività formative di ogni ordine e grado, nonché alle iniziative di orientamento, aggiornamento professionale ed inserimento nel mondo del lavoro erogate dall'Università degli Studi Roma Tre.

La presente informativa potrà essere soggetta ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/

Sommario

INFORMATIVA

L'Università degli studi Roma Tre, con sede in via Ostiense 159, 00154 Roma, Italia, C.F. e P.I. n. 04400441004 (di seguito, "**Università**"), in osservanza delle disposizioni del Regolamento UE 2016/679 (*General Data Protection Regulation*, di seguito "**GDPR**"), con il presente atto informa i soggetti interessati sulle modalità di trattamento dei dati personali raccolti. Per "**soggetti interessati"**, "**interessati**" o "**studenti**" si intendendo gli aspiranti studenti e studentesse, coloro che sono iscritti a qualsiasi corso di laurea e/o laurea magistrale, gli iscritti ai corsi singoli, ovvero a corsi *post lauream* (ad es. dottorato, scuola di specializzazione, corso di perfezionamento e master) nonché le persone che intendono partecipare a qualsiasi attività formativa (ad es. seminari, convegni, tirocini formativi, corsi di aggiornamento, etc.) ivi comprese le iniziative volte all'orientamento e all'assistenza all'inserimento nel mondo del lavoro.

Le informative relative ad altre categorie di interessati sono disponibili in allegato al Regolamento di Ateneo sulla privacy nonché all'indirizzo internet http:/www.uniroma3.it/privacy/.

TITOLARE DEL TRATTAMENTO

Titolare del trattamento dei dati personali è l'Università, come sopra definita, rappresentata dal Rettore *pro tempore*, domiciliato per la carica presso la sede della stessa. È possibile contattare il titolare del trattamento via e-mail scrivendo all'indirizzo privacy@uniroma3.it e PEC privacy@ateneo.uniroma3.it.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il responsabile della protezione dei dati ("**RPD**" o "**DPO**") è reperibile ai seguenti recapiti: e-mail rpd@uniroma3.it e PEC rpd@ateneo.uniroma3.it.

FINALITA' DEL TRATTAMENTO E BASE GIURIDICA

L'Università provvede alla raccolta e al trattamento dei dati personali degli interessati sulla base delle esigenze connesse allo svolgimento dei compiti istituzionali di pubblico interesse di cui è investita (ai fini della gestione del rapporto didattico e amministrativo con lo studente, anche con riferimento a specifici servizi dallo stesso richiesti, e per ogni altra finalità connessa all'erogazione dei servizi di istruzione, formazione, orientamento e assistenza all'inserimento nel mondo del lavoro), degli obblighi derivanti da un contratto con lo studente o dalla normativa vigente, nonché sulla base del consenso dei singoli interessati, ove necessario.

In particolare, l'Università tratta i dati per le seguenti finalità:

- erogazione dei servizi didattici e di segreteria studenti;
- organizzazione e svolgimento di iniziative volte all'orientamento in ingresso, in itinere ed in uscita;
- organizzazione di test di valutazione o ammissione a qualunque corso di formazione (ad es., corsi di studio, dottorati di ricerca, scuole di specializzazione, master, etc.);
- gestione della carriera universitaria;

- erogazione dei servizi per il diritto allo studio, delle borse di studio e di ricerca;
- organizzazione delle attività di collaborazione e dei tirocini extracurriculari;
- organizzazione delle procedure di partecipazione agli esami di stato;
- organizzazione delle elezioni studentesche e dei compiti inerenti le cariche elettive ricoperte negli organi dell'Università;
- erogazione dei servizi informatici e accesso ai laboratori e ad altre strutture protette;
- erogazione dei servizi bibliotecari;
- erogazione dei servizi di e-learning;
- erogazione di servizi di tutorato, assistenza, inclusione sociale;
- organizzazione e gestione delle attività sportive e culturali;
- sondaggi condotti anonimamente e su base aggregata;
- applicazione di procedimenti di natura disciplinare;
- coordinamento e organizzazione delle attività di *job placement*;
- gestione della sicurezza (ad es., gestione dei sistemi di videosorveglianza);
- adempimento degli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (cd. "amministrazione trasparente");
- previo ottenimento del consenso, per la comunicazione o diffusione, anche a privati, su richiesta dello studente, dei dati relativi agli esiti formativi, intermedi e finali, in conformità a quanto previsto dalla normativa applicabile.

In taluni casi il conferimento dei dati è obbligatorio in quanto necessario per il perseguimento delle finalità sopra menzionate, nonché all'adempimento di specifici obblighi di legge.

Infine, potranno essere trattati dati personali anche laddove ciò dovesse rendersi necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o per la gestione di eventuali reclami, per la repressione e il contrasto alle frodi e di qualsiasi altra attività illecita o perché richiesto dalle autorità competenti.

FONTI DEL TRATTAMENTO E CATEGORIE DI DATI

I dati personali dei soggetti interessati possono essere raccolti presso l'interessato (ad es., perché contenuti nella documentazione fornita all'atto dell'iscrizione o della richiesta di specifici servizi) oppure presso soggetti terzi (ad es. in caso di trasferimento ateneo, in caso di comunicazioni da altre istituzioni pubbliche o in caso di comunicazioni da università straniere, etc.) per il perseguimento di scopi istituzionali, in ottemperanza a specifici obblighi di legge, secondo l'interesse pubblico rilevante dell'Università o altra base giuridica.

Nello specifico, tra i dati trattati dall'Università vi rientrano le seguenti categorie di dati:

- dati comuni, quali i dati identificativi;
- dati particolari, quali i dati relativi allo stato di salute;
- dati giudiziari, intesi quali dati relativi a condanne penali, a reati o a connesse misure di sicurezza.

I dati raccolti potrebbero includere informazioni quali:

- dati identificativi, ivi inclusi, nome, cognome, genere, titolo, stato coniugale, indirizzo, paese di residenza, numero di telefono/fax, indirizzo e-mail, data e luogo di nascita, paese di nascita;
- dati relativi alla carriera universitaria (es. esami sostenuti, votazioni, etc.);

- dati relativi alla mobilità studentesca (es. adesione al programma Erasmus o ad altri scambi internazionali, votazioni conseguite per esami sostenuti all'estero etc.)
- informazioni contenute nella domanda di partecipazione ad eventuali procedure di selezione (es. borse di studio, di collaborazione o altre attività interne);
- dati reddituali (ad es., ISEE) e dati bancari (ad es. IBAN);
- immagini raccolte durante la registrazione delle lezioni, durante lo svolgimento di tornei, eventi sportivi o altre attività;
- immagini raccolte dalle telecamere di videosorveglianza (CCTV).

Inoltre, in aggiunta ai così detti dati comuni (quali, ad esempio, i dati identificativi dell'interessato), per le finalità di trattamento sopra indicate potranno essere raccolti e trattati, previa individuazione di idonea base giuridica o su istanza dell'interessato, particolari categorie di dati inerenti:

- l'origine razziale e etnica (ad es., per garantire i diritti spettanti ai cittadini extracomunitari e per lo status di rifugiato);
- dati particolari, quali i dati relativi allo stato di salute dei soggetti interessati (ad es., per assicurare i diritti spettanti agli studenti e studentesse diversamente abili o in stato di gravidanza);
- dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza, secondo quanto previsto dalla normativa vigente (ad es., per studenti e le studentesse sottoposti/e a misure restrittive della libertà personale);
- l'orientamento sessuale (nel caso di eventuali rettificazioni di attribuzione di sesso).

PERIODO DI CONSERVAZIONE DEI DATI

I dati personali inerenti alla carriera universitaria dello studente (es. iscrizione, esami sostenuti e relativi risultati, conseguimento del titolo di laurea) saranno conservati per un periodo di tempo illimitato, conformemente agli obblighi di archiviazione imposti dalla normativa vigente. I restanti dati personali raccolti saranno conservati dall'Università per il periodo di tempo necessario al conseguimento delle finalità per le quali sono raccolti e trattati o nei termini previsti da leggi, norme e regolamenti nazionali e comunitari a cui l'Università è tenuta ad attenersi (es. normativa di carattere contabile e fiscale, etc.).

DESTINATARI DEI DATI

I dati trattati per le finalità di cui sopra verranno trattati dal personale dell'Università, debitamente istruito e limitatamente a quanto necessario per l'espletamento dei rispettivi compiti. Ciò include, ad esempio, i docenti, i dipendenti e i collaboratori assegnati ai competenti uffici dell'Università, eventuali soggetti esterni che in qualità di incaricato prestano attività per conto dell'Università.

Inoltre, l'Università si avvale del supporto di fornitori esterni per l'erogazione di specifici servizi strumentali alla realizzazione delle proprie attività istituzionali. Tali soggetti sono nominati dall'Università quali Responsabili del Trattamento e possono accedere ai soli dati necessari e indispensabili per l'erogazione del servizio richiesto, secondo gli obblighi loro imposti dalla normativa vigente e dalle disposizioni contrattuali poste in essere dall'Università a garanzia della protezione dei dati personali. In particolare, trattano i dati degli interessati in tale veste:

- fornitori di servizi e/o prodotti informatici (es. sistemi per la gestione della carriera accademica e delle piattaforme di e-learning, assistenza agli utenti sull'utilizzo dei servizi, erogazione dei servizi di posta elettronica, conservazione dei dati, ecc.
- fornitori dei servizi di cassa e di tesoreria (es. per l'esecuzione dei mandati di pagamento);
- fornitori di servizi logistici per l'organizzazione di eventi, cerimonie, tornei sportivi o procedure di selezione;
- fornitori di servizi tecnico-amministrativi;
- fornitori di servizi assicurativi;
- consulenti e professionisti terzi (es. avvocati, commercialisti, ecc.).

Inoltre, l'Università può comunicare i dati personali di cui è titolare del trattamento ad altre amministrazioni pubbliche, qualora queste debbano trattare i medesimi per eventuali procedimenti di propria competenza istituzionale, nonché a tutti quei soggetti pubblici o privati ai quali, in presenza dei relativi presupposti, la comunicazione è prevista obbligatoriamente da disposizioni comunitarie, norme di legge o regolamento. Tali soggetti tratteranno i dati personali in qualità di autonomi titolari del trattamento. Pertanto, gli interessati potranno rivolgersi ad essi per far valere, ove applicabili, l'esercizio dei diritti di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità od opposizione. Tra questi soggetti sono compresi, a titolo esemplificativo e non esaustivo:

- soggetti pubblici che gestiscono l'erogazione di contributi di ricerca e/o borse di studio, che promuovono studi e ricerche, progetti per lo sviluppo universitario e servizi per il diritto allo studio;
- soggetti pubblici con finalità di sostegno all'inserimento nel mondo del lavoro, previa individuazione della più opportuna base giuridica per il trasferimento e adozione delle adeguate misure di pseudoanonimizzazione (ove necessario);
- soggetti terzi presso cui lo studente è chiamato a effettuare lo svolgimento di tirocini, *stage* o altre attività di *job placement*;
- amministrazioni statali, quali il Ministero dell'Istruzione, dell'Università e della Ricerca, il Ministero degli Affari Esteri, il Ministero del Lavoro, l'Agenzia delle Entrate, l'Avvocatura dello Stato, le Questure, le Ambasciate, le Procure della Repubblica, gli Istituti penitenziari;
- forze di polizia, l'autorità giudiziaria, gli organismi di informazione e sicurezza;
- enti pubblici non economici, quali INAIL ed enti previdenziali;
- società o consorzi partecipati dall'Università (ad es. CINEMA e Almalaurea)
- amministrazioni territoriali quali la Regione, l'Ente Regionale per il Diritto allo Studio e alla Conoscenza, la Direzione territoriale del lavoro, i Centri per l'Impiego, gli organismi regionali ed altri istituiti che forniscono servizi per il lavoro, orientamento e formazione professionale o che erogano sussidi e benefici economici;
- Atenei italiani e stranieri impegnati in percorsi formativi congiunti;
- associazioni, quale ad esempio la Conferenza dei Rettori delle Università Italiane – CRUI, enti e/o istituti in grado di favorire l'integrazione territoriale ed universitaria degli studenti e studentesse partecipamenti a scambi internazionali;
- aziende sanitarie locali;
- soggetti promotori e finanziatori di premi, borse ed assegni di studio e/o ricerca.

Al di fuori dei predetti casi, i dati personali non vengono in nessun modo e per alcun motivo comunicati o diffusi a terzi.

Infine, i dati personali degli interessati non sono generalmente oggetto di trasferimento verso Paesi o organizzazioni internazionali al di fuori del territorio dell'Unione Europea, salvo quando è necessario per l'erogazione di servizi di didattica e ricerca (es. università straniere nel caso di mobilità studentesca). Laddove i dati personali trattati dovessero essere trasferiti al di fuori del territorio dell'Unione Europea, tale trasferimento sarà compiuto esclusivamente sulla base dell'esistenza di garanzie appropriate e opportune secondo quanto previsto dal GDPR (es. Clausole Contrattuali Standard, iscrizione al Privacy Shield, etc).

DIRITTI DELL'INTERESSATO

Ogni interessato ha diritto di richiedere all'Università l'esercizio dei diritti previsti dal GDPR. In particolare, si tratta dei diritti di accesso, rettifica, cancellazione nonché del diritto alla portabilità dei dati, del diritto di limitazione del trattamento e del diritto di opposizione al trattamento, ove ne ricorrano i presupposti. Per ottenere maggiori informazioni sul trattamento dei propri dati personali o esercitare i suoi diritti, l'interessato ha diritto a contattare l'Università ai recapiti sopra indicati.

Di seguito è fornita una breve esplicazione dei diritti riconosciuti ai soggetti interessati dal trattamento:

- il diritto di accesso consente all'interessato di ottenere conferma che sia o meno in corso un trattamento dei suoi dati personali da parte dell'Università e, se del caso, accedere a tali dati e alle informazioni ad essi relative;
- il diritto di rettifica consente all'interessato di ottenere la modifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, di ottenere l'integrazione dei dati personali incompleti;
- il diritto alla cancellazione consente all'interessato di ottenere la cancellazione dei dati che lo riguardano senza ingiustificato ritardo (ad es. quando i suoi dati personali non sono più necessari in relazione alle finalità per cui sono stati raccolti), fatte salve le eccezioni previste dalla normativa applicabile (es. quando la conservazione dei dati è necessaria per il rispetto di obblighi di legge applicabili all'Università);
- il diritto alla portabilità dei dati consente all'interessato, in determinate circostanze previste dalla normativa, di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e che egli ha fornito all'Università.
- il diritto alla limitazione del trattamento consente all'interessato, in determinate circostanze previste dalla normativa, di ottenere la limitazione del trattamento dei propri dati personali.
- Il diritto di opposizione al trattamento consente all'interessato, in determinate circostanze previste dalla normativa, di opporsi al trattamento dei suoi dati personali. In tali casi l'Università si asterrà dal trattare ulteriormente i dati personali dell'interessato, salvo che l'Università stesso possa dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Inoltre, in qualsiasi momento, l'interessato ha il diritto di:

- revocare il consenso eventualmente prestato, senza con ciò pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- proporre reclamo al *Garante per la protezione dei dati personali* se ritiene che il trattamento che lo riguarda violi le disposizioni in materia di protezione dei dati personali.

INFORMATIVA PER IL PERSONALE

Informativa relativa al trattamento dei dati personali relativi alle persone fisiche che svolgono attività lavorative o di collaborazione, anche occasionale o di carattere professionale, per l'Università degli Studi Roma Tre.

La presente informativa potrà essere soggetta ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/

Sommario

INFORMATIVA

L'Università degli studi Roma Tre, con sede in via Ostiense 159, 00154 Roma, Italia, C.F. e P.I. n. 04400441004 (di seguito, "**Università**"), in osservanza delle disposizioni del Regolamento UE 2016/679 (*General Data Protection Regulation*, di seguito "**GDPR**"), con il presente atto, informa i soggetti interessati sulle modalità di trattamento dei dati personali raccolti. Per "**soggetti interessati**", "**interessati**" o **"lavoratori"** si intendono le persone fisiche aventi un rapporto di lavoro, anche a tempo determinato o di natura occasionale, con l'Università (ad esempio il personale docente, il personale tecnico, amministrativo e bibliotecario, i docenti a contratto, gli assegnisti di ricerca, i tutor nonché, limitatamente alle attività di collaborazione, gli studenti).

Le informative relative ad altre categorie di interessati sono disponibili in allegato al Regolamento di Ateneo sulla privacy nonché all'indirizzo internet http:/www.uniroma3.it/privacy/.

TITOLARE DEL TRATTAMENTO

Titolare del trattamento dei dati personali è l'Università, come sopra definita rappresentata dal Rettore *pro tempore*, domiciliato per la carica presso la sede della stessa. È possibile contattare il titolare del trattamento via e-mail scrivendo all'indirizzo privacy@uniroma3.it e PEC privacy@ateneo.uniroma3.it.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il responsabile della protezione dei dati ("**RPD**" o "**DPO**") è reperibile ai seguenti recapiti: e-mail rpd@uniroma3.it e PEC rpd@ateneo.uniroma3.it.

FINALITA' DEL TRATTAMENTO E BASE GIURIDICA

L'Università provvede alla raccolta e al trattamento dei dati personali degli interessati sulla base delle esigenze connesse allo svolgimento dei compiti istituzionali di pubblico interesse di cui è investita, delle esigenze precontrattuali e contrattuali, degli obblighi derivanti da un contratto o dalla normativa vigente, nonché sulla base del consenso dei singoli interessati, ove necessario.

In particolare, l'Università tratta i dati per le seguenti finalità:

- selezione del personale o affidamento di incarichi;
- gestione del rapporto di lavoro, ivi inclusi i trattamenti connessi all'adempimento agli obblighi relativi agli oneri fiscali e previdenziali nonché agli obblighi sanciti dalla contrattazione collettiva;
- gestione della carriera lavorativa;
- gestione di progetti di ricerca o di raccolta fondi;
- monitoraggio e valutazione della ricerca;
- attività di trasferimento tecnologico;
- erogazione di agevolazioni, servizi fiscali o qualsiasi iniziativa diretta a garantire la sicurezza e il benessere del personale (es. assegni familiari, rimborsi per asili nido e scuola, mobilità);
- gestione delle procedure elettive e dei compiti inerenti la carica elettiva ricoperta negli organi dell'Università;
- utilizzo dei servizi informatici e accesso ai laboratori e ad altre strutture protette;

- utilizzo dei servizi di telefonia fissa, mobile e di comunicazione;
- utilizzo dei servizi bibliotecari;
- organizzazione e gestione delle attività sportive e culturali;
- applicazione delle misure di sicurezza degli ambienti di lavoro;
- applicazione di procedimenti di natura disciplinare;
- gestione e amministrazione delle attività di formazione;
- monitoraggio della valorizzazione delle diversità e delle pari opportunità (nella misura consentita dalla normativa applicabile);
- sondaggi condotti anonimamente e su base aggregata;
- gestione della rubrica e degli elenchi interni all'Università, per la pubblicazione sulla Intranet o sui biglietti da visita di Ateneo o sulle comunicazioni all'esterno;
- gestione della sicurezza (ad es., gestione dei sistemi di videosorveglianza);
- adempimento degli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (cd. "amministrazione trasparente");
- amministrazione della mobilità dello staff (es. gestione viaggi, trasferte).

In taluni casi il conferimento dei dati è obbligatorio in quanto necessario per il perseguimento delle finalità sopra menzionate, nonché all'adempimento di specifici obblighi di legge.

Infine, potranno essere trattati dati personali anche laddove ciò dovesse rendersi necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o per la gestione di eventuali reclami, per la repressione e il contrasto alle frodi e di qualsiasi altra attività illecita o perché richiesto dalle autorità competenti.

FONTI DEL TRATTAMENTO E CATEGORIE DI DATI

I dati personali dei soggetti interessati possono essere raccolti presso l'interessato (ad es. all'atto della sottoscrizione del contratto o della richiesta di specifici servizi) oppure presso soggetti terzi (es. controllo delle autocertificazioni, acquisizione dall'INPS delle informazioni contenute nella Dichiarazione Sostitutiva Unica ai fini della concessione di agevolazioni, ecc.) per il perseguimento di scopi istituzionali, in ottemperanza a specifici obblighi di legge, secondo l'interesse pubblico rilevante dell'Università o altra base giuridica.

Nello specifico, tra i dati trattati dall'Università vi rientrano le seguenti categorie di dati:

- dati comuni, quali i dati identificativi;
- dati particolari, quali i dati relativi allo stato di salute;
- dati giudiziari, intesi quali dati relativi a condanne penali, a reati o a connesse misure di sicurezza.

I dati raccolti potrebbero includere informazioni quali:

- dati identificativi, ivi inclusi, nome, cognome, genere, titolo, stato coniugale, indirizzo, paese di residenza, numero di telefono/fax, indirizzo e-mail, data e luogo di nascita, contatti di emergenza, paese di nascita;
- dati contenuti nelle autocertificazioni trasmesse all'Università, nei certificati richiesti d'ufficio alle pubbliche amministrazioni che li detengono ordinariamente;
- ruolo, mansioni, orario di lavoro, orari di entrata e uscita, presenze, assenze, missioni, ferie programmate, etc.;

- dati oggetto di corrispondenza con gli uffici universitari (ivi incluse le domande concernenti l'Area competente per la gestione delle risorse umane);
- informazioni contenute nella domanda di assunzione e nei moduli di candidatura (ad esempio informazioni contenute nel CV, ivi incluse esperienze precedenti, informazioni relative all'istruzione, hobby e interessi, referenze, qualifiche accademiche e professionali);
- informazioni sulle performance dell'attività lavorativa (ivi incluse valutazioni, registri concernenti lo svolgimento di attività di formazione o di apprendimento);
- informazioni relative a procedimenti disciplinari;
- foto/immagini ottenute o scattate nell'ambito delle attività dell'Università;
- immagini raccolte dalle telecamere di videosorveglianza (CCTV)
- informazioni concernenti la remunerazione e i dettagli di conto bancario;
- dati fiscali e previdenziali;
- dettagli relativi a congedi di maternità, paternità e/o adozione;
- informazioni relative all'uso e all'accesso a sistemi informatici e informazioni relative ai dati di traffico telefonico;
- informazioni relative agli accessi a parcheggi o varchi riservati;
- dettagli forniti nelle notifiche di *whistleblowing*.

Inoltre, in aggiunta ai così detti dati comuni (quali, ad esempio, i dati identificativi dell'interessato), per le finalità di trattamento sopra indicate potranno essere raccolti e trattati, previa individuazione di idonea base giuridica o su istanza dell'interessato, particolari categorie di dati inerenti:

- dati particolari, quali i dati relativi allo stato di salute dei soggetti interessati, ivi incluse le informazioni rispetto alla malattia e alle disabilità;
- dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza, secondo quanto previsto dalla normativa vigente;
- l'orientamento sessuale (nel caso di eventuali rettificazioni di attribuzione di sesso);
- dati sull'appartenenza sindacale (quando rilevante, ad esempio per le ritenute sindacali.

PERIODO DI CONSERVAZIONE DEI DATI

I dati personali raccolti saranno conservati dall'Università per il periodo di tempo necessario al conseguimento delle finalità per le quali sono raccolti e trattati o nei termini previsti da leggi, norme e regolamenti nazionali e comunitari a cui l'Università è tenuta ad attenersi (es. normativa di carattere contabile e fiscale, etc.).

DESTINATARI DEI DATI

I dati trattati per le finalità di cui sopra verranno trattati dal personale dell'Università, debitamente istruito e limitatamente a quanto necessario per l'espletamento dei rispettivi compiti. Ciò include, ad esempio, i docenti, i dipendenti e i collaboratori assegnati ai competenti uffici dell'Università, eventuali soggetti esterni che in qualità di incaricato prestano attività per conto dell'Università.

Inoltre, l'Università si avvale del supporto di fornitori esterni per l'erogazione di specifici servizi strumentali alla realizzazione delle proprie attività istituzionali. Tali soggetti sono nominati dall'Università quali Responsabili del Trattamento e possono accedere ai soli dati necessari e indispensabili per l'erogazione del

servizio richiesto, secondo gli obblighi loro imposti dalla normativa vigente e dalle disposizioni contrattuali poste in essere dall'Università a garanzia della protezione dei dati personali. In particolare, trattano i dati degli interessati in tale veste:

- fornitori di servizi e/o prodotti informatici (es. sistemi per la gestione della carriera lavorativa e delle piattaforme di e-learning, assistenza agli utenti sull'utilizzo dei servizi, erogazione dei servizi di posta elettronica, conservazione dei dati, ecc.);
- fornitori dei servizi di cassa e di tesoreria (es. per l'esecuzione dei mandati di pagamento);
- fornitori di servizi logistici per l'organizzazione di cerimonie ed eventi e procedure di selezione;
- fornitori di servizi tecnico-amministrativi;
- fornitori di servizi assicurativi;
- consulenti e professionisti terzi (es. avvocati, commercialisti, ecc.).

Inoltre, l'Università può comunicare i dati personali di cui è titolare del trattamento ad altre amministrazioni pubbliche, qualora queste debbano trattare i medesimi per eventuali procedimenti di propria competenza istituzionale, nonché a tutti quei soggetti pubblici o privati ai quali, in presenza dei relativi presupposti, la comunicazione è prevista obbligatoriamente da disposizioni comunitarie, norme di legge o regolamento. Tali soggetti tratteranno i dati personali in qualità di autonomi titolari del trattamento. Pertanto, gli interessati potranno rivolgersi ad essi per far valere, ove applicabili, l'esercizio dei diritti di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità od opposizione. Tra questi soggetti sono compresi, a titolo esemplificativo e non esaustivo:

- amministrazioni statali, quali il Ministero dell'Istruzione, dell'Università e della Ricerca, il Ministero degli Affari Esteri, il Ministero del Lavoro, l'Agenzia delle Entrate, l'Avvocatura dello Stato, le Questure, le Ambasciate, le Procure della Repubblica, gli Istituti penitenziari;
- forze di polizia, l'autorità giudiziaria, gli organismi di informazione e sicurezza;
- enti pubblici non economici, quali INAIL ed enti previdenziali;
- società o consorzi partecipati dall'Università

Al di fuori dei predetti casi, i dati personali non vengono in nessun modo e per alcun motivo comunicati o diffusi a terzi.

Infine, i dati personali degli interessati non sono generalmente oggetto di trasferimento verso Paesi o organizzazioni internazionali al di fuori del territorio dell'Unione Europea. Laddove i dati personali trattati dovessero essere trasferiti al di fuori del territorio dell'Unione Europea, tale trasferimento sarà compiuto esclusivamente sulla base dell'esistenza di garanzie appropriate e opportune secondo quanto previsto dal GDPR (es. Clausole Contrattuali Standard, iscrizione al Privacy Shield, etc).

DIRITTI DELL'INTERESSATO

Ogni interessato ha diritto di richiedere all'Università l'esercizio dei diritti previsti dal GDPR. In particolare, si tratta dei diritti di accesso, rettifica, cancellazione nonché del diritto alla portabilità dei dati, del diritto di limitazione del trattamento e del diritto di opposizione al trattamento, ove ne ricorrano i presupposti. Per ottenere maggiori informazioni sul trattamento dei propri dati personali o esercitare i suoi diritti, l'interessato ha diritto a contattare l'Università ai recapiti sopra indicati.

Di seguito è fornita una breve esplicazione dei diritti riconosciuti ai soggetti interessati dal trattamento:

- il diritto di accesso consente all'interessato di ottenere conferma che sia o meno in corso un trattamento dei suoi dati personali da parte dell'Università e, se del caso, accedere a tali dati e alle informazioni ad essi relative;
- il diritto di rettifica consente all'interessato di ottenere la modifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, di ottenere l'integrazione dei dati personali incompleti;
- il diritto alla cancellazione consente all'interessato di ottenere la cancellazione dei dati che lo riguardano senza ingiustificato ritardo (ad es. quando i suoi dati personali non sono più necessari in relazione alle finalità per cui sono stati raccolti), fatte salve le eccezioni previste dalla normativa applicabile (es. quando la conservazione dei dati è necessaria per il rispetto di obblighi di legge applicabili all'Università);
- il diritto alla portabilità dei dati consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e che egli ha fornito all'Università.
- il diritto alla limitazione del trattamento consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di ottenere la limitazione del trattamento dei propri dati personali.
- Il diritto di opposizione al trattamento consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di opporsi al trattamento dei suoi dati personali. In tali casi l'Università si asterrà dal trattare ulteriormente i dati personali dell'interessato, salvo che l'Università stesso possa dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Inoltre, in qualsiasi momento, l'interessato ha il diritto di:

- revocare il consenso eventualmente prestato, senza con ciò pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- proporre reclamo al *Garante per la protezione dei dati personali* se ritiene che il trattamento che lo riguarda violi le disposizioni in materia di protezione dei dati personali.

INFORMATIVA PER I FORNITORI ED ENTI

Informativa relativa al trattamento dei dati personali relativi ad operatori economici interessati a partecipare a procedure di scelta del contraente per l'affidamento di forniture, servizi e l'esecuzione di lavori, ovvero a soggetti terzi, persone fisiche, che a vario titolo intrattengano rapporti con l'Università finalizzati al soddisfacimento delle esigenze delle strutture dell'Università nell'ambito dei propri fini istituzionali o per ricevere servizi resi dall'Università.

La presente informativa potrà essere soggetta ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/

Sommario

INFORMATIVA

L'Università degli studi Roma Tre, con sede in via Ostiense 159, 00154 Roma, Italia, C.F. e P.I. n. 04400441004 (di seguito, "**Università**"), in osservanza delle disposizioni del Regolamento UE 2016/679 (*General Data Protection Regulation*, di seguito "**GDPR**"), con il presente atto informa i soggetti interessati sulle modalità di trattamento dei dati personali raccolti. Per "**soggetti interessati**" o "**interessati**" si intendono le persone fisiche correlate ad ogni impresa e/o professionista che partecipi o che manifesti l'interesse a partecipare a procedure formali od informali di scelta del contraente, ovvero a altre persone fisiche che a vario titolo intrattengono rapporti di varia natura, non solo commerciale, con l'Università.

Le informative relative ad altre categorie di interessati sono disponibili in allegato al Regolamento di Ateneo sulla privacy nonché all'indirizzo internet http:/www.uniroma3.it/privacy/.

TITOLARE DEL TRATTAMENTO

Titolare del trattamento dei dati personali è l'Università, come sopra definita, rappresentata dal Rettore *pro tempore*, domiciliato per la carica presso la sede della stessa. È possibile contattare il titolare del trattamento via e-mail scrivendo all'indirizzo privacy@uniroma3.it e PEC privacy@ateneo.uniroma3.it.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il responsabile della protezione dei dati ("**RPD**" o "**DPO**") è reperibile ai seguenti recapiti: e-mail rpd@uniroma3.it e PEC rpd@ateneo.uniroma3.it.

FINALITA' DEL TRATTAMENTO E BASE GIURIDICA

L'Università provvede alla raccolta e al trattamento dei dati personali degli interessati sulla base delle esigenze connesse allo svolgimento dei compiti istituzionali di pubblico interesse di cui è investita, delle esigenze precontrattuali e contrattuali, degli obblighi derivanti da un contratto o dalla normativa vigente, nonché sulla base del consenso dei singoli interessati, ove necessario.

In particolare, l'Università tratta i dati per le seguenti finalità:

- fornitura di beni e servizi (ad es. per accertare l'esistenza dei requisiti richiesti ai fini della partecipazione a procedure di scelta del contraente, o per verificare l'esistenza dei presupposti di legge per poter contrarre con la pubblica amministrazione);
- stipula di contratti e convenzioni;
- gestione delle iniziative accademiche, formative e di inserimento nel mondo del lavoro con partner dell'Università, compresi attività di inserimento lavorativo (es. *job placement*), stage e ogni altra attività formativa correlata;
- attivazione tirocini curriculari, formativi e di orientamento;
- informazione, comunicazione e realizzazione di attività di orientamento in itinere e di orientamento al lavoro;
- informazione, comunicazione e realizzazione di eventi e attività di *job placement*;
- pagamento dei corrispettivi delle prestazioni rese in favore dell'Università a qualunque titolo;

- consentire l'accesso alle strutture dell'Università ed il supporto alle attività istituzionali, ivi compresa la raccolta di fondi;
- gestione dei rapporti con i soggetti terzi che interagiscono con il personale universitario o con gli studenti;
- adempimento degli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (cd. "amministrazione trasparente").

In taluni casi il conferimento dei dati è obbligatorio in quanto necessario all'espletamento delle procedure e/o al perfezionamento del contratto, nonché all'adempimento di specifici obblighi di legge.

Infine, potranno essere trattati dati personali anche laddove ciò dovesse rendersi necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o per la gestione di eventuali reclami, per la repressione e il contrasto alle frodi e di qualsiasi altra attività illecita o perché richiesto dalle autorità competenti.

FONTI DEL TRATTAMENTO E CATEGORIE DI DATI

I dati personali dei soggetti interessati possono essere raccolti presso l'interessato (ad es. all'atto della sottoscrizione del contratto o della richiesta di specifici servizi), presso l'ente di afferenza oppure presso soggetti terzi (ad es. ANAC, SICEANT, Camera di commercio, INPS, INAIL, Cassa Edile), per il perseguimento di scopi istituzionali, in ottemperanza a specifici obblighi di legge, secondo l'interesse pubblico rilevante dell'Università o altra base giuridica.

Nello specifico, tra i dati trattati dall'Università vi rientrano le seguenti categorie di dati:

- dati comuni, quali i dati identificativi;
- dati giudiziari, intesi quali dati relativi a condanne penali, a reati o a connesse misure di sicurezza.

I dati raccolti potrebbero includere informazioni quali:

- dati identificativi, ivi inclusi, nome, cognome, genere, titolo, stato coniugale, indirizzo, paese di residenza, numero di telefono/fax, indirizzo e-mail, data e luogo di nascita, contatti di emergenza, paese di nascita;
- ruolo all'interno dell'ente di afferenza;
- iscrizioni al Registro Imprese o altri dati contenuti in registri pubblici;
- informazioni contenute nella domanda di partecipazione ad una procedura di selezione;
- immagini raccolte dalle telecamere di videosorveglianza (CCTV);
- informazioni concernenti i dettagli di conto bancario;
- informazioni relative agli accessi a parcheggi o varchi riservati.

Inoltre, in aggiunta ai così detti dati comuni (quali, ad esempio, i dati identificativi dell'interessato), per le finalità di trattamento sopra indicate potranno essere raccolti e trattati, previa individuazione di idonea base giuridica o su istanza dell'interessato, particolari categorie di dati inerenti:

- dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza, secondo quanto previsto dalla normativa vigente.

PERIODO DI CONSERVAZIONE DEI DATI

I dati personali raccolti saranno conservati dall'Università per il periodo di tempo necessario al conseguimento delle finalità per le quali sono raccolti e trattati o nei termini previsti da leggi, norme e regolamenti nazionali e comunitari a cui l'Università è tenuta ad attenersi (es. normativa di carattere contabile e fiscale, etc.).

DESTINATARI DEI DATI

I dati trattati per le finalità di cui sopra verranno trattati dal personale dell'Università, debitamente istruito e limitatamente a quanto necessario per l'espletamento dei rispettivi compiti. Ciò include, ad esempio, i docenti, i dipendenti e i collaboratori assegnati ai competenti uffici dell'Università, eventuali soggetti esterni che in qualità di incaricato prestano attività per conto dell'Università.

Inoltre, l'Università si avvale del supporto di fornitori esterni per l'erogazione di specifici servizi strumentali alla realizzazione delle proprie attività istituzionali. Tali soggetti sono nominati dall'Università quali Responsabili del Trattamento e possono accedere ai soli dati necessari e indispensabili per l'erogazione del servizio richiesto, secondo gli obblighi loro imposti dalla normativa vigente e dalle disposizioni contrattuali poste in essere dall'Università a garanzia della protezione dei dati personali. In particolare, trattano i dati degli interessati in tale veste:

- fornitori di servizi e/o prodotti informatici (es. sistemi per la gestione degli albi fornitori, sistemi di conservazione dei dati, ecc.);
- fornitori dei servizi di cassa e di tesoreria (es. per l'esecuzione dei mandati di pagamento);
- fornitori di servizi logistici per l'organizzazione di cerimonie ed eventi e procedure di selezione;
- fornitori di servizi tecnico-amministrativi;
- fornitori di servizi assicurativi;
- consulenti e professionisti terzi (es. avvocati, commercialisti, ecc.).

Inoltre, l'Università può comunicare i dati personali di cui è titolare del trattamento ad altre amministrazioni pubbliche, qualora queste debbano trattare i medesimi per eventuali procedimenti di propria competenza istituzionale, nonché a tutti quei soggetti pubblici o privati ai quali, in presenza dei relativi presupposti, la comunicazione è prevista obbligatoriamente da disposizioni comunitarie, norme di legge o regolamento. Tali soggetti tratteranno i dati personali in qualità di autonomi titolari del trattamento. Pertanto, gli interessati potranno rivolgersi ad essi per far valere, ove applicabili, l'esercizio dei diritti di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità od opposizione. Tra questi soggetti sono compresi, a titolo esemplificativo e non esaustivo:

- amministrazioni statali, quali il Ministero dell'Istruzione, dell'Università e della Ricerca, il Ministero degli Affari Esteri, il Ministero del Lavoro, l'Agenzia delle Entrate, l'Avvocatura dello Stato, le Questure, le Ambasciate, le Procure della Repubblica, gli Istituti penitenziari;
- forze di polizia, l'autorità giudiziaria, gli organismi di informazione e sicurezza;
- enti pubblici non economici, quali INAIL ed enti previdenziali;
- società o consorzi partecipati dall'Università

Al di fuori dei predetti casi, i dati personali non vengono in nessun modo e per alcun motivo comunicati o diffusi a terzi.

Infine, i dati personali degli interessati non sono generalmente oggetto di trasferimento verso Paesi o organizzazioni internazionali al di fuori del territorio dell'Unione Europea. Laddove i dati personali trattati dovessero essere trasferiti al di fuori del territorio dell'Unione Europea, tale trasferimento sarà compiuto esclusivamente sulla base dell'esistenza di garanzie appropriate e opportune secondo quanto previsto dal GDPR (es. Clausole Contrattuali Standard, iscrizione al Privacy Shield, etc).

DIRITTI DELL'INTERESSATO

Ogni interessato ha diritto di richiedere all'Università l'esercizio dei diritti previsti dal GDPR. In particolare, si tratta dei diritti di accesso, rettifica, cancellazione nonché del diritto alla portabilità dei dati, del diritto di limitazione del trattamento e del diritto di opposizione al trattamento, ove ne ricorrano i presupposti. Per ottenere maggiori informazioni sul trattamento dei propri dati personali o esercitare i suoi diritti, l'interessato ha diritto a contattare l'Università ai recapiti sopra indicati.

Di seguito è fornita una breve esplicazione dei diritti riconosciuti ai soggetti interessati dal trattamento:

- il diritto di accesso consente all'interessato di ottenere conferma che sia o meno in corso un trattamento dei suoi dati personali da parte dell'Università e, se del caso, accedere a tali dati e alle informazioni ad essi relative;
- il diritto di rettifica consente all'interessato di ottenere la modifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, di ottenere l'integrazione dei dati personali incompleti;
- il diritto alla cancellazione consente all'interessato di ottenere la cancellazione dei dati che lo riguardano senza ingiustificato ritardo (ad es. quando i suoi dati personali non sono più necessari in relazione alle finalità per cui sono stati raccolti), fatte salve le eccezioni previste dalla normativa applicabile (es. quando la conservazione dei dati è necessaria per il rispetto di obblighi di legge applicabili all'Università);
- il diritto alla portabilità dei dati consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e che egli ha fornito all'Università.
- il diritto alla limitazione del trattamento consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di ottenere la limitazione del trattamento dei propri dati personali.
- Il diritto di opposizione al trattamento consente all'interessato, in determinate circostanze previste dalla normativa applicabile, di opporsi al trattamento dei suoi dati personali. In tali casi l'Università si asterrà dal trattare ulteriormente i dati personali dell'interessato, salvo che l'Università stesso possa dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Inoltre, in qualsiasi momento, l'interessato ha il diritto di:

- revocare il consenso eventualmente prestato, senza con ciò pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- proporre reclamo al *Garante per la protezione dei dati personali* se ritiene che il trattamento che lo riguarda violi le disposizioni in materia di protezione dei dati personali.

INFORMATIVA SINTETICA ED ALTRE

INFORMATIVE SPECIFICHE

Informativa sintetica (da utilizzare ove non sia possibile fornire la stessa in maniera completa) ed eventuali altre informative relative a trattamenti specifici. Le presenti informative potranno essere soggette ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/.

INFORMATIVA SINTETICA

L'Università degli studi Roma Tre ("**Università**"), con sede in via Ostiense 159, 00154 Roma, Italia, C.F. e P.I. n. 04400441004, in osservanza delle disposizioni del Regolamento UE 2016/679 ("**GDPR**"), con il presente atto informa i soggetti interessati circa i trattamenti posti in essere, le relative finalità e modalità di trattamento dei dati personali raccolti. Una versione completa e aggiornata dell'informativa è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/.

TITOLARE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

Titolare del trattamento dei dati personali è l'Università, rappresentata dal Rettore *pro tempore*. È possibile contattare il titolare del trattamento via e-mail scrivendo all'indirizzo privacy@uniroma3.it e PEC privacy@ateneo.uniroma3.it.

Il responsabile della protezione dei dati ("**RPD**" o "**DPO**") è reperibile ai seguenti recapiti: e-mail rpd@uniroma3.it e PEC rpd@ateneo.uniroma3.it.

FINALITA' DEL TRATTAMENTO, BASE GIURIDICA E PERIODO DI CONSERVAZIONE

L'Università provvede alla raccolta e al trattamento dei dati personali degli interessati sulla base delle esigenze connesse allo svolgimento dei compiti istituzionali di pubblico interesse di cui è investita, delle esigenze precontrattuali e contrattuali, degli obblighi derivanti da un contratto o dalla normativa vigente, nonché sulla base del consenso dei singoli interessati, ove necessario. Tra i trattamenti posti in essere dall'Università, vi rientrano:

- i dati degli studenti, ad esempio in relazione alle attività di didattica, alla gestione della carriera, ai servizi bibliotecari, alle borse di studio etc;
- i dati dei visitatori delle strutture dell'Università che non hanno alcun rapporto con la stessa, ad esempio in relazione alle attività di videosorveglianza;
- i dati dei dipendenti, ad esempio relativamente alle attività svolte, ai propri congedi di malattia, etc.;
- i dati dei fornitori, collaboratori e altri soggetti che prestano attività per conto dell'Università.

I dati personali raccolti saranno conservati dall'Università per il periodo di tempo necessario al conseguimento delle finalità per le quali sono raccolti e trattati o nei termini previsti da leggi, norme e regolamenti nazionali e comunitari. Per quanto concerne i trattamenti di videosorveglianza, i dati saranno trattati in loco e il tempo di conservazione delle immagini non eccederà i 7 giorni (salvo specifiche esigenze, quali l'avvenimento di un illecito o la presenza di una richiesta da parte delle autorità).

DESTINATARI DEI DATI

L'Università potrebbe trasmettere alcun dati personali raccolti nell'ambito delle proprie attività di trattamento a soggetti esterni nominati responsabili del trattamento o ad altre amministrazioni pubbliche o privati, ove consentito (es. soggetti che gestiscono erogazione di contributi di ricerca o studio, enti con finalità di *job placement*.

DIRITTI DELL'INTERESSATO

Ogni interessato ha diritto di richiedere all'Università l'esercizio dei diritti previsti dal GDPR. In particolare, si tratta dei diritti di accesso, rettifica, cancellazione nonché del diritto alla portabilità dei dati, del diritto di limitazione del trattamento e del diritto di opposizione al trattamento, ove ne ricorrano i presupposti. È altresì possibile proporre reclamo al *Garante per la protezione dei dati personali* se si ritiene che il trattamento che lo riguarda violi le disposizioni in materia di protezione dei dati personali.

ISTRUZIONI PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI

Sono fornite di seguito le istruzioni necessarie a garantire il corretto trattamento dei dati personali in coerenza con gli obiettivi dell'Università perseguiti e nel rispetto dei principi generali in materia di protezione dei dati personali che devono essere rispettati da tutti i dipendenti o collaboratori a qualsiasi titolo in qualità di incaricati.

Le istruzioni potranno essere soggette ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/.

Sommario

PREMESSA

Scopo del documento

Nell'ottica di un efficace tutela delle informazioni e dei dati personali gestiti dall'Università degli Studi Roma Tre, il presente documento ha lo scopo di fornire le prescrizioni e le istruzioni circa il complesso delle misure organizzative, logistiche, tecniche, ed informatiche da adottare in tutte le strutture dell'Università, affinché il livello di protezione dei dati personali oggetto di trattamento sia conforme, nel quadro dei più generali obblighi di sicurezza, a quanto previsto dal Regolamento UE 2016/679 (*General Data Protection Regulation*, di seguito "*GDPR*") e dal *Regolamento in materia di protezione dei dati personali* (di seguito "*Regolamento"*), e sia tale in ogni caso da garantire attraverso un trattamento lecito e corretto gli interessi e i diritti fondamentali dell'interessato. Le istruzioni presenti nel documento potranno essere integrate dal titolare del trattamento o dal responsabile interno del trattamento con indicazioni più dettagliate riferite ad uno specifico trattamento.

Principi guida dell'azione amministrativa

Il diritto alla protezione dei dati personali mira a garantire che il trattamento delle informazioni si svolga "nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali". Il principio guida dell'azione amministrativa è rappresentato pertanto dal "principio di necessità del trattamento", il quale, assieme ai correlati principi di "pertinenza e non eccedenza", rappresenta un presupposto di liceità del trattamento medesimo. I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Livelli adeguati di sicurezza

Nell'ambito del predetto obbligo generale il titolare del trattamento e il responsabile interno del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso

a) la pseudonimizzazione e la cifratura dei dati personali,
b) la capacità di assicurare su base permanente la riservatezza[1], l'integrità[2], la disponibilità[3] e la resilienza[4] dei sistemi e dei servizi di trattamento,

[1] La capacità di garantire l'accesso protetto e controllato ai dati solo alle persone effettivamente autorizzate a garanzia della confidenzialità delle informazioni trattate
[2] La capacità di garantire la consistenza e la protezione dei dati nei confronti di modifiche, accidentali (involontarie) oppure effettuate volontariamente da una terza parte.
[3] La capacità di continuare a trattare dati, nei tempi e nei luoghi previsti, anche a seguito di un incidente o di un evento esterno imprevisto.

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico,
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il titolare del trattamento e il responsabile interno del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso.

[4] La capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati.

OBBLIGHI

Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'Università e alle informazioni che la stessa ha comunicato agli interessati, nonché alle mansioni previste dal contratto di lavoro dell'incaricato. In particolare, devi:

- raccogliere e trattare esclusivamente i dati necessari e sufficienti al corretto svolgimento delle tue proprie mansioni. L'eventuale raccolta dei dati deve avvenire nel rispetto delle procedure e dei modelli di informazione e/o consenso elaborati dall'Università e disponibili nel Regolamento;
- acquisire il consenso dell'interessato laddove previsto;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalle vigenti disposizioni in materia di protezione dei dati personali;
- prestare particolare attenzione all'esattezza dei dati trattati e provvedere all'aggiornamento e all'integrazione degli stessi nell'ambito delle proprie attribuzioni;
- provvedere con la dovuta diligenza affinché non vengano conservati dati personali non pertinenti, non necessari o divenuti superflui;
- informare il responsabile interno del trattamento in merito alle richieste degli interessati e supportarlo nella corretta evasione delle stesse, in conformità al Regolamento;
- assicurare che i Responsabili del Trattamento esterni siano vincolati dagli obblighi imposti dal GDPR, adottando le misure contrattuali indicate nel Regolamento e inserendo una clausola a tale scopo nei contratti di fornitura sottoscritti;
- in caso di una violazione che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, informare tempestivamente il responsabile interno del trattamento e/o direttamente il responsabile della protezione dei dati e cooperare con lo stesso nella gestione della violazione;
- eseguire esclusivamente le operazioni di trattamento a cui sei autorizzato/a attenendoti alle istruzioni ricevute e alle misure di sicurezza indicate e nel rispetto delle procedure interne dell'Università.

In conclusione, devi utilizzare i dati personali solo per le finalità connesse allo svolgimento delle tue mansioni lavorative, con divieto di qualsiasi altra diversa utilizzazione. L'utilizzo dei dati personali deve avvenire in base al principio del "need to know" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati personali devono essere trattati nella misura strettamente necessaria e sufficiente per le finalità previste e per il periodo necessario a tali fini. I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi se non previa autorizzazione.

Accesso ad archivi cartacei o a banche dati

Le disposizioni e gli obblighi in materia di archivi pubblici sono indifferentemente riferibili ad ogni ente pubblico, pertanto, in base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, devi:

- accedere esclusivamente agli archivi/banche dati per effettuare i trattamenti strettamente pertinenti alle mansioni svolte e per le finalità previste dal titolare del trattamento, rispettando i principi fondamentali delle regolamentazioni di legge in materia e del Regolamento;
- astenerti dall'accedere ad archivi/banche dati diversi da quelli indicati, nonché realizzare nuove ed autonome banche dati con finalità diverse da quelle consentite (es. laddove compili dei fogli excel con dati di studenti per finalità proprie o comunque diverse da quelle previste per la tua mansione);
- astenerti dal trasportare al di fuori dei luoghi di lavoro i documenti cartacei/ elettronici (o copia degli stessi) senza specifica autorizzazione, salvo i casi di comunicazione dei dati a terzi autorizzati dall'Università;
- impedire che estranei, o in ogni caso terzi non autorizzati, prendano conoscenza dei dati personali non a loro riferibili;
- sviluppare misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, e adottando, in presenza di specifici rischi, particolari cautele;
- tutelare l'integrità degli archivi e l'autenticità dei documenti, anche elettronici e multimediali, in particolare di quelli esposti a rischi di cancellazione, dispersione ed alterazione dei dati;
- salvaguardare la conformità delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;
- astenerti dal fare alcun uso delle informazioni non disponibili agli utenti o non rese pubbliche, ottenute in ragione della propria attività anche in via confidenziale, per proprie ricerche o per realizzare profitti e interessi privati;
- mantenere riservate i dati personali, notizie e informazioni ad essi concernenti apprese nell'esercizio delle proprie attività, osservando tali doveri di riserbo anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro;
- classificare e fascicolare correttamente tutti i documenti protocollati:
    - a norma dell'art. 52 del DPR 445/2000, il sistema di protocollo informatico deve fornire anche le indicazioni sul collegamento esistente tra ciascun documento ricevuto e i documenti prodotti dall'amministrazione nello svolgimento del relativo procedimento amministrativo, fino all'eventuale provvedimento finale. Il fascicolo informatico è lo strumento che consente l'aggregazione dei documenti all'interno del sistema di protocollo informatico in base al procedimento e nel rispetto del vincolo archivistico;
    - a norma degli artt. 67, 68 e 69 del DPR 445/2000, almeno una volta ogni anno, il Responsabile di ciascuna UOR, provvede a trasferire nell'archivio di deposito tutta la documentazione relativa ai procedimenti conclusi, rispettando l'organizzazione che i fascicoli avevano nell'archivio corrente e i criteri di scarto/conservazione permanente dei documenti, anche al fine di garantire che i dati vengano conservati per il periodo strettamente necessario al conseguimento delle finalità per le quali sono raccolti e trattati

o nei termini previsti da leggi, norme e regolamenti nazionali e comunitari a cui l'Università è tenuta ad attenersi.

Responsabilità

Ti ricordo che il trattamento dei dati personali effettuato in difformità alle finalità e modalità previste può configurare le ipotesi di responsabilità disciplinate dalla vigente normativa in materia di lavoro e tutela della privacy; pertanto devi:

- compiere tutto quanto sia necessario e adottare tutte le iniziative e gli interventi idonei a garantire il rispetto delle vigenti disposizioni in materia di protezione dei dati personali;
- segnalare tempestivamente ogni eventuale problema relativo all'adempimento degli obblighi previsti dalle vigenti disposizioni in materia di protezione dei dati personali.

Più in generale, dovrai garantire il pieno rispetto delle norme vigenti in materia di trattamento, attenerti alle istruzioni indicate nel Regolamento e ad ogni altra indicazione ricevuta dal titolare del trattamento o dal responsabile per la protezione dei dati.

ISTRUZIONI OPERATIVE

Come posso sapere se è consentito compiere un determinato trattamento?

Innanzitutto, assicurati che il trattamento che stai per compiere sia sussumibile sotto uno dei trattamenti indicati nelle informative presenti all'indirizzo http://www.uniroma3.it/privacy/.
Se il trattamento è indicato all'interno dell'informativa, puoi procedere con il trattamento in quanto l'Università ha già compiuto le proprie valutazioni in merito all'idonea base giuridica per poter procedere con il trattamento. Se il trattamento che intendi compiere non è indicato tra quelli presenti nelle informative, passa alla prossima domanda.

Posto che il trattamento non è indicato nelle Informative, posso comunque eseguirlo?

Se un trattamento non è sussumibile sotto uno dei trattamenti indicati nelle informative presenti all'indirizzo http://www.uniroma3.it/privacy/, ciò non significa che non possa essere eseguito. Tuttavia, prima di poter cominciare il trattamento sarà necessario (1) individuare l'idonea base giuridica e (2) dare immediata comunicazione del nuovo trattamento al responsabile interno del trattamento e al DPO affinché quest'ultimo possa inserirlo nelle informative sulla protezione dei dati personali pubblicate online dall'Università.
Per individuare l'idonea base giuridica del trattamento occorre distinguere tra dati personali così detti "comuni", dati particolari (o così detti "dati sensibili") e dati relativi a condanne penali, reati o misure di sicurezza (così detti "dati giudiziari"). Fai riferimento alle definizioni contenute nel regolamento di Ateneo per capire in quale categorie rientrano i dati che intendi trattare. Ciò detto, a seconda della categoria, potrai trattare i dati solo se sussiste una delle seguenti condizioni:

- Per quanto concerne i dati personali afferenti alla categoria dei dati "comuni", sussiste una base giuridica per procedere con il trattamento se:
    - il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (ad esempio, l'interessato è una persona fisica che agisce quale fornitore e il trattamento è necessario per consentire all'Università di adempiere agli obblighi espressamente indicati nel contratto); oppure
    - il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (ad esempio, c'è una norma di legge che espressamente impone all'Università di eseguire il trattamento); oppure
    - il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (ad esempio, uno studente, si trova all'estero in una condizione di assoluta emergenza, come un attacco terroristico in corso, e si presume che la sua vita o quella di un'altra persona possa essere in pericolo se non si procede al trattamento, quale, ad esempio, fornire allo stesso dei recapiti telefonici); oppure

- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (ad esempio, il trattamento rientra nell'ambito dei servizi di pubblica istruzione che costituiscono vocazione dell'Università, o in altro dei trattamenti individuati espressamente dal Codice Privacy o da altra norma di legge); oppure
- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (ad esempio, l'interessato ha fatto una specifica richiesta in tal senso).

Il consenso dell'interessato, quale base giuridica del trattamento, deve essere acquisito solo ed esclusivamente nei casi in cui non sia individuabile una diversa base giuridica per procedere al trattamento.

- Per quanto concerne i dati personali afferenti alla categoria dei dati "sensibili", sussiste una base giuridica per procedere con il trattamento se:
  - il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto italiano, dell'UE o da un contratto collettivo, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; oppure
  - il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; oppure
  - il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato (da interpretarsi in modo stringente); oppure
  - il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria dinanzi una autorità con funzioni giurisdizionali; oppure
  - il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto italiano o del diritto UE, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; oppure
  - il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto italiano o dell'UE; oppure
  - il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, secondo quanto previsto dal diritto italiano o dell'UE, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; oppure
  - l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo che la normativa disponga comunque che detto trattamento non possa compiersi.

Il consenso dell'interessato, quale base giuridica del trattamento, deve essere acquisito solo ed esclusivamente nei casi in cui non sia individuabile una diversa base giuridica per procedere al trattamento.

- Per quanto concerne i dati personali afferenti alla categoria dei dati "giudiziari", sussiste una base giuridica per procedere con il trattamento se:
    - il trattamento è espressamente autorizzato dal diritto italiano o dell'UE, e tale norma prevede garanzie appropriate per i diritti e le libertà degli interessati. Se tale base giuridica si fonda su un'autorizzazione generale del Garante per la protezione dei dati personali, dovrà scrupolosamente accertarsi che detta autorizzazione sia vigente e applicabile al caso concreto. Inoltre, si ricorda che il trattamento dei dati "giudiziari" non può trovare fondamento nel meccanismo del consenso.

Una volta individuata la pertinente base giuridica del trattamento, tenendo conto delle indicazioni sopra fornite e della normativa applicabile, si prega di informare tempestivamente il proprio responsabile interno del trattamento e il DPO, affinché quest'ultimo possa darne menzione nelle informative di cui all'indirizzo http://www.uniroma3.it/privacy/.

Cosa fare se dati personali sono stati sottratti, comunicati o diffusi a persone terze non autorizzate?

Devi eseguire scrupolosamente la *procedura di notifica della violazione di dati personali* descritta nel Regolamento.

Conserva sempre il consenso rilasciato dall'interessato

Laddove sia necessario raccogliere il consenso, occorre predisporre misure organizzative e tecniche atte a garantire la conservazione della copia del consenso acquisito, sia esso cartaceo o elettronico, da parte della struttura autorizzata al trattamento; in particolare:

- il consenso richiede una dichiarazione o un'azione positiva inequivocabile da parte dell'interessato, il che significa che il consenso deve sempre essere espresso attraverso una dichiarazione o in modo attivo. Pertanto è vietato predisporre moduli in cui la casella di acquisizione del consenso (c.d. "check-box") risulta pre-compilata con lo specifico simbolo (c.d. flag),
- qualora il consenso sia espresso in formato elettronico è opportuno memorizzare quante più informazioni utili relativamente all'operazione eseguita dall'interessato: data e ora, indirizzo IP di provenienza, sistema operativo e nome utente, ecc.,
- qualora il consenso sia espresso in formato cartaceo occorre conservare la copia cartacea per la durata utile del trattamento e oltre la cessazione del trattamento ove previsto da regolamenti di ateneo o dalla normativa vigente.

Gestisci la distanza di cortesia

Il ricevimento degli utenti va organizzato in modo da evitare che persone terze, dipendenti o meno, possano, anche involontariamente, ascoltare i colloqui che ciascun utente intrattiene con il personale

addetto a recepire le relative istanze. Deve, cioè, essere garantita la così detta *distanza di cortesia* nelle ipotesi in cui vengano in rilievo dati personali dell'interessato.

Non comunicare dati personali a soggetti non legittimati

L'utilizzo dei dati personali deve avvenire in base al così detto "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative. I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi, se non previa autorizzazione del responsabile interno del trattamento nelle ipotesi consentite dalla normativa vigente.

Utilizza le chiavi

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone, se non altro, un primo ostacolo e richiede comunque uno sforzo volontario non banale per la sua rimozione.
È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sfogliare i documenti posti su una scrivania; pertanto:

- chiudi a chiave il tuo ufficio quando l'ultima unità di personale lascia il locale,
- non lasciare i documenti incustoditi sul tavolo, ma riponili in fascicoli non immediatamente accessibili,
- alla fine della giornata chiudi i documenti a chiave nei cassetti o negli armadi ogni volta che puoi.

Cura la spedizione dei documenti

Il trasferimento di ogni documento contenente dati personali deve seguire rigorose misure di garanzia, tali da impedire che allo stesso accedano estranei: buste chiuse e sigillate, invio con raccomandata di ritorno, non abbandono durante i trasferimenti.
Tali accortezze possono essere ridotte qualora si utilizzi il servizio postale interno all'Università; resta comunque valida l'accortezza di imbustare i documenti per non renderli immediatamente accessibili.

Conserva i documenti cartacei nel modo corretto

Esamina le modalità di archiviazione delle informazioni valutando se ne hai ancora bisogno e se il luogo di conservazione permette l'accesso solo al personale autorizzato.
I documenti da conservare devono essere gestiti in modo da poter essere rintracciati e individuati facilmente, se necessario. I documenti contenenti dati sensibili devono essere conservati in armadietti chiusi a chiave il cui accesso è limitato a un determinato numero di persone all'interno dell'Università.

Fai attenzione a come distruggi i documenti

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili. Anche eventuali fotocopie mal riuscite di documenti contenenti dati

personali devono essere distrutte. I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Archivistica.

Non lasciare in vista documenti

In caso di riunione nella tua stanza, di ricevimento di utenti o ancora se lavori presso uno sportello informativo, fai sempre attenzione ai documenti presenti sulla tua postazione di lavoro.
Assicurati di rimuoverli e di archiviarli per tempo per evitare che chiunque possa accedere a informazioni personali.

Raddoppia le attenzioni se i documenti contengono dati particolarmente sensibili

I documenti contenenti dati particolarmente sensibili devono essere controllati e custoditi molto attentamente in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di certificati medici, permessi sindacali, condanne penali, ecc., deve avvenire per il tempo strettamente necessario e, subito dopo, i documenti devono essere archiviati.
L'archiviazione dei documenti cartacei deve avvenire possibilmente in locali ad accesso controllato, utilizzando armadi o contenitori chiusi a chiave. Per accedere agli archivi fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione oppure farsi identificare e registrare su appositi registri.

Non dimenticare le stampe dei documenti

Stampare un documento e dimenticarsi di averlo fatto può costituire un rischio per la sicurezza. Non lasciare accedere alle stampe o ai fax persone non autorizzate; se la stampante o il fax non si trova sulla tua scrivania recati quanto prima a ritirare le stampe.
Sincerati inoltre che al momento dello spegnimento del computer non vi siano documenti in coda di stampa.

Limita l'uso di supporti di memorizzazione portatili

I supporti di memorizzazione portatili, quali CD, DVD, chiavette USB, dischi esterni, ecc. rappresentano un potenziale rischio per la perdita dei dati. Difatti qualora vengano smarriti o sottratti chiunque vi acceda può comunicare o diffondere dati personali a persone terze non autorizzate. È pertanto fortemente consigliato utilizzare i sistemi di comunicazione, memorizzazione e condivisione dei dati messi a disposizione dall'Università quali la posta elettronica, OneDrive, Filesender e SharePoint[5]. Per i supporti di memorizzazione elettronica si applicano gli stessi criteri dei documenti cartacei: riponeteli negli armadi o nei cassetti non appena avete finito di usarli e non lasciateli incustoditi sul tavolo.

La password è personale

La password o i dispositivi di autenticazione (badge, dispositivi OTP, cellulare, ecc.) sono strettamente personali e non devono essere a conoscenza o prestati a nessun altro utente all'infuori del proprietario. Se

[5] Si rimanda all'appendice per la descrizione di tali strumenti.

hai il sospetto che qualcuno possa essere venuto a conoscenza della tua password, cambiala immediatamente.

Non comunicare mai la tua password a seguito di una mail

Spesso succede di ricevere messaggi di posta elettronica, SMS o comunicazioni social, nelle quali un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile quale una banca, un fornitore di servizi informatici o addirittura un collega di lavoro. Il messaggio imita nell'aspetto e nel contenuto messaggi legittimi e richiede di fornire soldi o informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio.
Ricorda che nessuno è autorizzato a conoscere la tua password, neanche i tecnici informatici e tantomeno a chiedertela tramite posta elettronica: non rispondere per alcun motivo al messaggio e cancellalo.

Utilizza le password in modo corretto

Vi sono differenti categorie di password, ognuna con il proprio ruolo preciso:

- la password di accesso al computer impedisce l'utilizzo improprio della tua postazione, quando per un motivo o per l'altro non ti trovi in ufficio,
- la password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio,
- la password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato,
- la password del salvaschermo, infine, impedisce che una tua assenza momentanea permetta a una persona non autorizzata di visualizzare il tuo lavoro.

Imposta o chiedi ai tecnici informatici che venga sempre impostata una password.

Blocca sempre i dispositivi informatici quando non li utilizzi

Ogni qual volta devi sospendere il lavoro sullo strumento informatico, assicurati che lo stesso sia bloccato e che non vi si possa accedere se non digitando la relativa password o PIN.

Non farti sbirciare quando digiti le password

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digiti la tua password, questa potrebbe essere letta guardando i tasti che stai battendo sulla tastiera, anche se hai buone capacità di dattiloscrittura. Assicurati che non ci sia nessuno nelle vicinanze che possa carpire la password.
Analogamente sui dispositivi touch (tablet, smartphone, ecc.) il codice PIN digitato per lo sblocco del dispositivo o la password possono essere facilmente individuati a partire dalle porzioni dello schermo sulle quali si depositano le impronte. Per ridurre il rischio, pulisci spesso lo schermo e sostituisci frequentemente la pellicola salvaschermo.

Custodisci le password in un luogo sicuro

Non scrivere la tua password, meno che mai vicino alla tua postazione di lavoro. L'unico dispositivo di registrazione affidabile è la tua memoria. Se hai necessità di conservare traccia delle password per scritto, non lasciare in giro i fogli utilizzati.

Applica lo stesso criterio anche per le credenziali di firma elettronica dei documenti.

Scegli bene la tua password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è parte essenziale della sicurezza informatica. Utilizza password che sia per te facile da ricordare (legata ad esempio alla vita personale non conosciuta dagli altri) che abbia le seguenti caratteristiche:

- deve essere obbligatoriamente cambiata almeno ogni 3/6 mesi,
- lunghezza minima di otto caratteri (consigliata almeno 12),
- deve contenere almeno una lettera maiuscola,
- deve contenere almeno una lettera minuscola,
- deve contenere almeno un numero,
- deve contenere almeno un carattere speciale (es $, #, ?, !, ecc.),
- deve essere diversa dalle ultime tre utilizzate.

Per ogni account usa password differenti

Non utilizzate mai la password della mail per altri account, ad esempio quelli social; qualora venisse violata la password del profilo social i truffatori avrebbero l'accesso anche alla tua mail. Per quanto possibile utilizza password diverse per ogni servizio on-line cui sei registrato.

Cosa non devi fare con la tua password

- NON dire a nessuno la tua password. Ricorda che lo scopo principale per cui utilizzi una password è assicurare che nessun altro possa utilizzare le tue risorse o possa farlo a tuo nome. Non comunicarla neanche ai tecnici informatici incaricati dell'assistenza sul tuo pc e ove assolutamente indispensabile, procedi immediatamente dopo a cambiarla,
- NON usare il tuo nome o cognome: è la password più semplice da indovinare,
- NON usare password che possano in qualche modo essere legate a te che possono essere facilmente conosciute come, ad esempio, il nome del coniuge o dei figli, del cane, date di nascita, numeri di telefono ecc.

Presta attenzione all'utilizzo dei personal computer portatili o tablet

I personal computer portatili e i tablet sono un facile bersaglio per i furti. Se hai necessità di gestire dati riservati su un portatile, chiedi l'installazione di un buon programma di cifratura del disco rigido oppure utilizza i sistemi di comunicazione, memorizzazione e condivisione dei dati messi a disposizione dall'Università quali la posta elettronica, OneDrive, Filesender e SharePoint in modo da limitare i dati personali sul dispositivo.

Non utilizzare dispositivi non autorizzati

I dispositivi di accesso (computer, tablet, smartphone, modem, ecc.) rappresentano un punto di accesso sia alla rete che ai dati trattati. Pertanto, è necessario che su di essi vengano applicate le misure minime

previste al fine di garantirne la sicurezza e l'integrità. L'utilizzo di dispositivi personali o non autorizzati viola le politiche di sicurezza definite dall'Università; ad esempio:

- l'utilizzo di modem o di hot-spot wi-fi su postazioni di lavoro collegati alla rete dell'Università offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata,
- l'utilizzo di computer personali o di supporti di memorizzazione portatili personali (chiavette usb, dischi esterni, CD, ecc.) può rappresentare un veicolo per la diffusione di virus e la conseguente perdita di dati.

Non installare programmi non autorizzati

Solo i programmi istituzionali o acquistati dall'Università con regolare licenza sono autorizzati. Se il tuo lavoro richiede l'utilizzo di programmi specifici, consulta i tecnici autorizzati ad effettuare l'assistenza sul tuo PC.

Non utilizzare strumenti di comunicazione, memorizzazione e condivisione non autorizzati

Oggi è facile creare account "personali" per usufruire di servizi di comunicazione (es Gmail, Yahoo Mail, Hotmail, ecc.), di memorizzazione e condivisione (GoogleDrive, Dropbox, WeTransfer, ecc.). Si tratta appunto di account "personali" legati alla propria persona e in fase di attivazione del servizio il fornitore non ha alcun obbligo di riservatezza in riferimento a dati che non riguardano colui che ha attivato l'account. A ciò si aggiunge che, per rispettare quanto previsto dal GDPR, il fornitore del servizio deve essere nominato responsabile del trattamento. Pertanto, trasferire su tali sistemi dati personali riguardanti, ad esempio, dati anagrafici degli studenti, rappresenta una violazione delle norme sulla privacy.
È pertanto vietato:

- inoltrare la posta elettronica ricevuta sull'indirizzo istituzionale (xxxx@uniroma3.it o xxx@yyy.uniroma3.it) verso altri indirizzi di posta elettronica (ad esempio privati, o di aziende presso le quali si sta svolgendo contemporaneamente altra attività lavorativa),
- memorizzare o condividere file utilizzando piattaforme (ad esempio GoogleDrive, Dropbox, WeTransfer, ecc.) diverse da quelle istituzionali.

Applica con cura le linee guida per la prevenzione da infezioni di virus

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati o nella divulgazione di dati personali a terzi.

Diffida delle mail sospette

Diffida dalle mail che contengono fatture di servizi, prodotti mai acquistati o documenti provenienti dalla pubblica amministrazione senza posta certificata. Se hai effettuato un acquisto, attendi una spedizione o una fattura ma l'email sembra sospetta, contatta direttamente il fornitore per verificarla.

Contrassegna l'email di phishing come posta indesiderata, in questo modo futuri invii dello stesso tipo saranno intercettati automaticamente e non ti saranno riproposti.

Non utilizzare la mail istituzionale per la registrazione a servizi personali

L'email malevole possono anche non avere dei fini economici diretti, in molti casi vengono inviate anche solo per prendere il controllo del vostro pc, per utilizzarlo a vostro nome per effettuare altri attacchi o accedere all'interno di una rete. Per questo non dovete utilizzare la vostra mail istituzionale per iscrivervi a servizi on-line di e-banking, e-commerce, ai social network, forum e blog; esponete l'Università e i vostri dati a nuovi rischi.

Fai attenzione a come distruggi i supporti di memorizzazione

I supporti di memorizzazione (chiavette usb, dischi esterni, CD, DVD, dichi rigidi, ecc.) contenenti dati personali devono essere cancellati in modo definitivo prima di essere ceduti a terzi o smaltiti.
La semplice cancellazione dei file (ad esempio effettuata con il tasto "CANC") da un supporto di memoria o la formattazione di un hard disk non significa che le informazioni registrate siano cancellate per sempre. Spesso, queste ultime rimangono fisicamente presenti e tecnicamente recuperabili. Inoltre, bisogna considerare che dati personali possono essere contenuti anche in apparecchi elettronici apparentemente insospettabili: ad esempio, le moderne fotocopiatrici, i fax e le stampanti sono dotate di un hard disk interno simile a quello che si trova nei PC e nei laptop. Questi apparecchi memorizzano automaticamente qualsiasi documento che sia stato fotocopiato o stampato e possono quindi contenere dati personali da distruggere al momento della loro dismissione o reimpiego.
Qualora non sia possibile cancellare in modo permanente i dati da un dispositivo, questo deve essere distrutto.

Ricordati di fare sempre il backup

I dati possono essere cancellati per diverse cause: involontariamente, con l'esecuzione di operazioni errate, a causa di virus, a seguito di furto, per verificarsi di calamità naturali, ecc. Per tale motivo chi dispone di dati personali su supporto informatico deve provvedere periodicamente ad eseguire le cosiddette copie di salvataggio (backup) delle informazioni che si intende proteggere da indebita o volontaria cancellazione. Il salvataggio dei dati va effettuato con cadenza almeno settimanale ed è obbligatorio qualora i dati in questione non siano disponibili presso altri sistemi informatici. Difatti l'Università è tenuta al ripristino dell'accesso ai dati in caso di danneggiamento degli stessi, in tempi certi compatibili con i diritti degli interessati. Si consiglia quindi l'utilizzo di strumenti di memorizzazione messi a disposizione dall'Università.

Dove puoi posizionare i server

Nel caso di trattamento informatico, devono essere attivate, se non già operative, procedure di controllo d'accesso alle sale in cui sono ubicati server e ai locali dove sono ubicati gli altri sistemi informatici utilizzati per il trattamento di dati personali. Evitate di installare server che contengono dati personali all'interno della propria stanza o in zone facilmente accessibili a chiunque.

ISTRUZIONI OPERATIVE PER IL WEB

Cancella fisicamente i file dal server web

Ricordati che i file pubblicati, seppur non più collegati all'interno della pagina web, sono sempre raggiungibili dai motori di ricerca. Ricordati quindi di cancellare fisicamente i file dal server e non limitarti a rimuovere semplicemente il link dalla pagina.

Non pubblicare gli esiti degli esami

Non pubblicare esiti degli esami o delle prove intermedie. Per pubblicare queste informazioni, utilizza il sistema di gestione delle carriere degli studenti che consente di pubblicare o inviare comunicazioni solo ai diretti interessati.

Limita le informazioni pubblicate nelle graduatorie

Qualora sia necessario pubblicare dati personali sul web utilizza per quanto possibile sistemi che consentano l'accesso alle informazioni solo attraverso le credenziali di autenticazione che hanno tutte le studentesse, gli studenti e il personale. Se proprio non è possibile utilizzare questi strumenti, ove non sussistano altre norme di pubblicità o trasparenza, limitati a pubblicare solo il cognome e nessun'altro dato personale (nome, data, luogo di nascita, codice fiscale, ISEE, IBAN, dati di domicilio/residenza, recapiti telefonici/email, ecc.).

Se è proprio necessario caricare ulteriori dati personali, contatta il responsabile interno del trattamento per definire le modalità di pubblicazioni e quali informazioni devono prima essere oscurate.

In ogni caso rimuovi fisicamente il file pubblicato sul web una volta che non è più necessario ai fini del procedimento che si è concluso.

Ricordati inoltre che:

- nel d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, sono contenute specifiche indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni,
- sul sito del Garante sono pubblicate le *Linee guida per il trattamento di dati personali effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web* che rappresentano un utile riferimento nell'individuare contenuti, modalità ed eccezioni relativamente alla pubblicazione di dati personali sul web.

Non pubblicare mai documenti con le firme autografe

Per garantire l'accessibilità dei documenti pubblicati, anche da persone con disabilità, è indispensabile pubblicare il file originario (word, excel, ecc.) convertito in formato pdf. Un documento di testo acquisito mediante scansione, anche se in formato pdf, è inaccessibile e pertanto non deve essere pubblicato. Eventualmente al documento originario, prima di essere convertito in pdf, può essere aggiunta l'indicazione (F.to) accanto al nominativo del firmatario – ad esempio (F.to) Mario Rossi – o la dicitura: "Il presente documento, conforme all'originale, è conservato negli archivi ...", indicando l'ufficio competente alla conservazione del documento stesso.

Non devono essere mai pubblicati documenti contenenti firme autografe o la scansione di firme autografe.

ISTRUZIONI OPERATIVE PER LA VIDEO SORVEGLIANZA

Tutte le immagini che contengono informazioni relative a persone fisiche e ne consentono l'identificazione anche indirettamente o mediante riferimenti sono classificate "DATI PERSONALI". Pertanto, in materia di videosorveglianza, la consultazione, la conservazione, l'estrapolazione, la manipolazione e la cancellazione, sono tutte operazioni che costituiscono un trattamento di dati.
Il personale autorizzato che ha accesso alle immagini in diretta o registrate ha l'obbligo di mantenere riservati i dati durante ciascuna operazione di trattamento.

Posiziona correttamente il cartello

Il cartello "informativa" deve essere accessibile e chiaramente visibile a tutti gli interessati rispettando determinate caratteristiche: esso deve essere posizionato prima del raggio di azione della telecamera o nelle sue immediate vicinanze, non necessariamente a contatto con gli impianti. Deve essere chiaramente visibile e riconoscibile mediante il suo formato e collocamento, in ogni condizione di illuminazione ambientale, anche in orario notturno.

Limita la visuale di ripresa

Il trattamento di dati mediante l'uso delle apparecchiature volte a riprendere ("Telecamere"), con o senza registrazione delle immagini, deve essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti per non incorrere nel reato penale di "Interferenze illecite nella vita privata". Resta anche vietato l'utilizzo di telecamere finte.

Proteggi i monitor e i registratori

Il monitor di controllo presente presso i siti videosorvegliati o in una sala operativa centralizzata, deve essere posizionato in un luogo sicuro, presidiato e in modo da non consentire che terzi possano sbirciare, fotografare o video-riprendere le immagini rappresentate su di esso.
Le modalità di protezione dei DVR/NVR sono le medesime utilizzate per i server che trattano dati personali. È altresì necessario adottare le misure di sicurezza preventive come password complesse, criptazione dei dati e altri strumenti disponibili, durante i processi di conservazione e manipolazione delle immagini.

Cancella i supporti

Inoltre, prima della dismissione dei dispositivi e comunque in tutti i casi ove la presenza delle immagini non sia più utile, è importante accertarsi che i supporti di memorizzazione siano stati cancellati definitivamente e i filmati siano irrecuperabili.

La diffusione è vietata

I dati personali relativi alla videosorveglianza possono essere utilizzati esclusivamente per quelle che sono le finalità per cui è stato attivato il trattamento. È assolutamente vietato darne diffusione a soggetto alcuno, anche se dipendente dell'Università, ad eccezione dei dati ceduti su specifico ordine, alle Autorità Giudiziarie a fini investigativi.

ISTRUZIONI OPERATIVE PER I SOCIAL NETWORK

Per Social Network, si intende un gruppo di persone connesse tra di loro sia a livello umano che a livello virtuale attraverso "piattaforme sociali" il cui scopo principale è la conoscenza, lo scambio di informazioni, di risorse e quant'altro. Tra le più utilizzate a livello mondiale possiamo citare: Facebook, Twitter, Instagram e LinkedIn.

L'identificazione non è sicura

Non comunicare attraverso i social informazioni personali, ma utilizza sempre gli strumenti ufficiali dell'Università per identificare il destinatario della comunicazione (posta elettronica di ateneo, cellulare di servizio). L'interlocutore si potrebbe celare dietro false identità per carpire in modo illegittimo dati personali altrui. Identifica l'interessato esclusivamente con sistemi basati sul riconoscimento diretto o sicuro prima dar seguito alle sue richieste.

Non pubblicare alcun dato personale

La pubblicazione di dati personali (elenchi nominativi, voti, valutazioni didattiche, foto, filmati, pensieri ecc.) è irreversibile. Nonostante la volontà di rimuoverli dai social, i contenuti, se già diffusi, resteranno illimitatamente nella rete. Prima di condividere qualsiasi dato, riferito a soggetti terzi o a te stesso, fai la massima attenzione. Evita che i dati personali possano finire nelle mani sbagliate.

Disattiva la Geo-localizzazione

Per quanto ormai diffusa la moda di postare nei social, foto, video, posizione geocartografica dei luoghi che visitiamo, è consigliato farlo solo nella fase successiva al rientro dal viaggio, in modo da evitare che eventuali malfattori, a conoscenza dell'assenza dall'abitazione e dal luogo di lavoro, possano approfittarne per commettere azioni criminose ed entrare in possesso oltre che di oggetti, documenti o dispositivi che contengono i dati personali propri o altrui.

ISTRUZIONI OPERATIVE PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a "riprodursi" senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmette un virus:

- attraverso l'installazione di programmi provenienti da fonti non ufficiali o non autorizzate,
- attraverso la copia di dati da supporti di memorizzazione (USB, hard disk, ecc.),
- attraverso le macro presenti nei file dei programmi di automazione d'ufficio (Office, OpenOffice, ecc.),
- attraverso dati o programmi che si scaricano da Internet.

Come non si trasmette un virus:

- attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.),
- attraverso mail non contenenti allegati.

Come prevenire i virus:

1. usa soltanto programmi provenienti da fonti fidate: copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati,
2. evita di collegare al tuo computer supporti di memorizzazione (USB, hard disk, ecc.): infatti se il supporto di memorizzazione fosse infettato, il virus si trasferirebbe nel computer e potrebbe contagiare ad altri file,
3. proteggi i tuoi supporti di memorizzazione da scrittura quando possibile: in questo modo eviterai le scritture accidentali, magari tentate da un virus. I virus non possono in ogni caso aggirare la protezione meccanica,
4. assicurati che il tuo software antivirus sia aggiornato: la tempestività nell'azione di contrasto è essenziale per limitare i danni che un virus può causare ed è pertanto è vitale che il programma antivirus sia aggiornato e che conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Gli aggiornamenti sono rilasciati, di solito, con frequenza almeno giornaliera,
5. non diffondere messaggi di provenienza dubbia: se ricevi messaggi che avvisano di un nuovo virus pericolosissimo, ignoralo: messaggi di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"),
6. non partecipare a "catene di s. antonio" e simili: tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*, aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

Per qualsiasi dubbio, o per ulteriori informazioni, prima di installare qualsiasi programma o aprire qualsiasi mail sospetta, contatta i tecnici autorizzati ad effettuare l'assistenza sul tuo computer.

INFORMAZIONI SUGLI STRUMENTI DI COLLABORAZIONE DISPONIBILI

L'Ateneo mette a disposizione dei suoi utenti (studenti e personale) strumenti di collaborazione per la condivisione di informazioni, quali:

- Filesender: applicazione web per l'invio facile e sicuro di file di grandi dimensioni,
- FindTime: piattaforma per confrontare le disponibilità e trovare l'orario migliore per organizzare una riunione (un servizio analogo a Premium Doodle),
- IBM Connections: piattaforma con una serie di strumenti (blog, chat, forum, wiki, profili, like e commenti) che aumentano l'efficienza comunicativa e collaborativa tra colleghi
- OneDrive: spazio disco da 5 TB per la gestione di documenti con gruppi di lavoro (un servizio analogo a DropBox, GoogleDrive, ecc),
- Outlook: casella di posta elettronica da 100 GB,
- SharePoint: ambiente di collaborazione per la condivisione di documenti, attività, processi, etc.,
- Skype: strumento di comunicazione e collaborazione per realizzare chat, video conferenze anche contemporaneamente con più utenti (di ateneo o di altre organizzazioni) dalla propria postazione di lavoro o con il proprio smartphone,
- Yammer: piattaforma di Social Network dedicata per personale universitario e studenti.

L'impiego di questi strumenti aumenta la sicurezza dei dati, pertanto per quanto possibile utilizzali. Di seguito trovi le informazioni sui alcuni di questi strumenti, per qualsiasi ulteriore delucidazione puoi contattare i tecnici informatici incaricati dell'assistenza sul tuo pc.

Filesender

Si tratta di un'applicazione web che permette agli utenti di inviare a qualsiasi destinatario, in modo facile e sicuro, file molto grandi ovviando ai limiti solitamente imposti alla posta elettronica.

I file inviati vengono caricati su un'area di storage temporanea e restano disponibili per il download per un periodo di tempo limitato, dopodiché vengono automaticamente cancellati. La sicurezza è garantita perché solo i legittimi destinatari sono in grado di scaricare i file: ogni volta che verrà scaricato, al mittente verrà inviata una notifica via e-mail. È possibile inviare file a qualsiasi indirizzo di posta elettronica, anche non universitario. Il servizio permette anche la ricezione di file da utenti non in possesso delle credenziali di ateneo, o di una università o ente federato in IDEM.

Il servizio può essere utilizzato solo per l'invio di file e non costituisce una piattaforma di storage o di pubblicazione permanente. FileSender è utilizzabile da tutti gli utenti delle organizzazioni aderenti alla Federazione GARR (Università ed Enti di Ricerca).

Per utilizzare FileSender GARR basta collegarsi all'indirizzo: https://filesender.garr.it selezionare il nome dell'organizzazione (Università degli studi Roma Tre) ed effettuare il login con le credenziali di ateneo.

OneDrive

OneDrive è un servizio di *file hosting* sviluppato da Microsoft che connette l'utente a tutti i file. Consente di archiviare in un'unica posizione i tuoi file personali fino ad 1 TB, condividerli con altri utenti (interni od esterni all'Università) e accedervi ovunque si trovino in tutti i dispositivi.

Tutti i file archiviati in OneDrive sono privati a meno che non decidi di condividerli. È possibile condividere file e cartelle con i colleghi in modo da poter collaborare ai progetti, ma anche con partner esterni all'Università. Quando si inviano messaggi di posta elettronica dalla webmail, è possibile allegare un file di OneDrive come collegamento, invece di inviare il file vero e proprio: in questo caso è possibile assegnare automaticamente ai destinatari del messaggio l'autorizzazione per la modifica o meno del file e la data sino alla quale il file resterà disponibile.

È inoltre possibile sincronizzare il contenuto di OneDrive su diversi dispositivi in modo da accedere ai file in piena mobilità: ad oggi è possibile collegare dispositivi con sistema operativo Windows, MacOS, Android o iOS.

OneDrive conserva automaticamente la cronologia di tutte le revisioni effettuate sui file, pertanto è possibile ripristinare le versioni precedenti. Inoltre OneDrive rappresenta un backup dei propri file: difatti in caso di furto, distruzione o sostituzione del proprio dispositivo è possibile recuperare tutti i file dal cloud.

Outlook

L'Università mette a disposizione un servizio cloud di posta elettronica: oltre alle normali funzioni di ricezione e invio della posta, è possibile i calendari degli altri utenti per pianificare le riunioni, prenotare le sale riunioni, programmare video conferenze.

Sharepoint

SharePoint è una piattaforma software di Content Management System (CMS) sviluppata da Microsoft, ovvero permette la creazione di siti web principalmente ad uso interno per condividere documenti e altre informazioni. È possibile creare liste, repository documentali, attività, calendari sincronizzati con Outlook e altro. Dal momento che tutte le informazioni sono salvate su server, è possibile lavorare su di essi in collaborazione, ricevere notifiche ogni qual volta un utente ha modificato un file, condividere commenti e post, definire workflow di approvazione, ricercare documenti, il tutto assegnando a ciascun gruppo di utenti profili differenti (utenti che possono solo visualizzare, oppure modificare i contenuti, ecc).

Si tratta quindi di uno strumento che aggiunge alle funzionalità di condivisione dei file (già presenti in OneDrive) ulteriori funzionalità che consente l'interazione e la collaborazione tra utenti.

PROCEDURA DI NOTIFICA DELLE VIOLAZIONI

Procedura operativa da applicare qualora un incaricato del trattamento verifichi o abbia sospetto di una violazione dei dati personali.

La presente procedura potrà essere soggetta ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/.

Sommario

1. NOTIFICA AL RESPONSABILE DELLA PROTEZIONE DEI DATI

1. Qualora si verifichi una violazione dei dati personali, l'incaricato del trattamento coinvolto informa tempestivamente e con qualsivoglia mezzo il proprio responsabile interno del trattamento e/o il responsabile della protezione dei dati subito dopo essere venuto a conoscenza della violazione. Inoltre, l'incaricato del trattamento è contestualmente tenuto ad inviare al responsabile della protezione dei dati una e-mail, contrassegnata come urgente, avente il seguente oggetto: "URGENTE – VIOLAZIONE DATI PERSONALI [NOME UFFICIO]". Tale comunicazione è dovuta in ogni caso, a prescindere che il responsabile della protezione dei dati sia già stato informato o meno.
2. L'email deve contenere una descrizione quanto più possibile dettagliata di:
    a. natura della violazione
    b. tipologie di dati e interessati coinvolti
    c. indicazione della portata della violazione (in termini numerici)
    d. misure eventualmente adottate
3. Il responsabile della protezione dei dati provvede a convocare, se necessario, una riunione con gli interlocutori interessati al fine di acquisire maggiori informazioni ed eventualmente decidere le azioni successive.

2. NOTIFICA AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

1. L'Università notifica la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, salvo che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati. Il titolare del trattamento adotta i provvedimenti del caso sentito il parere del Direttore Generale, del Dirigente competente a seconda degli uffici coinvolti dalla violazione e del responsabile della protezione dei dati.
2. I soggetti sopra elencati valutano le azioni da intraprendere tenuto conto delle indicazioni fornite dalle competenti strutture informatiche (se del caso) e dai risultati dell'indagine interna condotta dal responsabile della protezione dei dati ai sensi del Regolamento di Ateneo.
3. Qualora la notifica al Garante non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
4. La notifica all'Autorità di Controllo deve contenere almeno i seguenti elementi:
    a. descrivere la natura della violazione compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
    c. descrivere le probabili conseguenze della violazione;
    d. descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.
5. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni devono essere fornite in fasi successive senza ritardo.

3. NOTIFICA AGLI INTERESSATI

1. Quando la violazione presentare potenzialmente un rischio elevato per i diritti e le libertà degli Interessati, l'Università comunica la violazione all'interessato, anche in questo caso senza ingiustificato ritardo.
2. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione e contiene almeno le seguenti informazioni e misure:
    a. l'indicazione del nome e i dati di contatto del soggetto interno all'Università presso cui è possibile ottenere più informazioni sull'incidente;
    b. una descrizione delle probabili conseguenze della violazione;
    c. la descrizione delle misure adottate, o di cui si propone l'adozione da parte del titolare del trattamento, per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.
3. Non è richiesta la comunicazione all'interessato in questione se è soddisfatta una delle seguenti condizioni:
    a. siano state attuate le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
    b. siano state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
    c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, l'Università deve procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. I soggetti di cui al paragrafo 2.1 valutano la sussistenza delle circostanze per le quali non è necessario notificare agli interessati l'avvenuta Violazione.

CLAUSOLE STANDARD

Sono fornite di seguito facsimili di clausole da utilizzare nella documentazione fornita agli interessati (studenti e studentesse, personale o terzi che intraprendono rapporti con l'Università).

Le clausole potranno essere soggette ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/

Sommario

Informativa

L'Informativa sul trattamento dei dati personali è un documento che deve essere fornito dal titolare del trattamento (cioè, il soggetto che singolarmente o insieme ad altri determina le finalità e i mezzi del trattamento di dati personali).

La seguente clausola deve essere inserita ogni qual volta vengano raccolti dati presso l'interessato (studente/studentessa, personale, fornitore od ente) da parte dell'Università, in qualità di titolare del trattamento (ad esempio, attraverso la compilazione di moduli cartacei o online, la stipula di convenzioni o contratti, etc.).

Bandi:

Art. XX - Informativa

L'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 è pubblicata sul sito www.uniroma3.it/privacy/.

Modulistica cartacea:

Con la sottoscrizione del presente documento dichiaro di aver preso visione dell'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito www.uniroma3.it/privacy/.

Modulistica cartacea/online:

☐ *Dichiaro di aver preso visione dell'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito www.uniroma3.it/privacy/.*

Modulistica online:

*Cliccando sul pulsante "**[inserire il nome del pulsante come, ad esempio, "Continua", "Invia", etc.]**" dichiaro di aver preso visione dell'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito www.uniroma3.it/privacy/.*

Consenso al trattamento (dati personali di tipo comune)

Poiché l'Università tratta dati personali prevalentemente per adempiere ad un obbligo giuridico o perché il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri di cui è investita, il consenso degli interessati non è generalmente necessario. Infatti, il consenso rappresenta soltanto una delle tante basi giuridiche su cui può trovare fondamento un trattamento di dati personali. Di conseguenza, la seguente dicitura dovrebbe essere utilizzata esclusivamente in casi marginali, laddove la raccolta del consenso è strettamente necessaria in quanto non è possibile individuare una differente base giuridica per il trattamento (es. non è ravvisabile la presenza di un obbligo contrattuale, di un interesse pubblico rilevante, ecc.). Le modalità di individuazione della base giuridica del trattamento sono indicate nell'*Allegato 5 - Istruzioni per il corretto trattamento dei dati personali*.

In alcuni casi particolari, quali, ad esempio, la comunicazione o diffusione a terzi dei dati relativi agli esiti formativi, intermedi e finali, al fine di favorire l'inserimento nel mondo del lavoro, potrebbe essere necessario predisporre una specifica informativa e raccogliere il consenso dell'interessato.

Si ricorda che in questi casi:

- non è possibile ricorrere al principio del silenzio-assenso: l'autorizzazione deve essere espressa in modo esplicito. Ove si utilizzino sistemi informatici si raccomanda di registrare puntualmente tutte le informazioni associate al consenso (data, ora, indirizzo IP, ecc.)
- il consenso non può essere "suggerito" dal sistema di raccolta dei dati. Ad esempio, nel caso si utilizzino sistemi informatici, l'opzione "Acconsento" non deve essere selezionata per default (es. pre-spuntata), ma deve essere libera e lasciata alla incondizionata ed esplicita selezione da parte dell'interessato.

Modulistica cartacea/online:

☐ *Dichiaro di aver preso visione dell'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito www.uniroma3.it/privacy e acconsento al trattamento dei miei dati personali per le finalità ivi indicate.*

Modulistica online:

*Cliccando sul pulsante "**[inserire il nome del pulsante come, ad esempio, "Continua", "Invia", etc.]**" dichiaro di aver preso visione dell'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito www.uniroma3.it/privacy/ e acconsento al trattamento dei miei dati personali per le finalità ivi indicate.*

Consenso al trattamento (categorie particolari di dati personali)

Poiché l'Università tratta dati personali prevalentemente per adempiere ad un obbligo giuridico o perché il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri di cui è investita, il consenso degli interessati non è generalmente necessario. Infatti, il consenso rappresenta soltanto una delle basi giuridiche su cui può trovare fondamento un trattamento di dati personali appartenente alle categorie particolari di dati (cioè, quei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona).

Mentre in molti casi un consenso specifico non è necessario (ad esempio, per gestire i certificati medici dei lavoratori assenti per malattia), in alcuni casi potrebbe essere necessario predisporre una specifica informativa e raccogliere il consenso dell'interessato. Di conseguenza, si fornisce di seguito un modulo di consenso, ricordando che tale dicitura dovrà fornirsi in aggiunta all'eventuale consenso richiesto per i cd. dati comuni e comunque sempre priva di pre-selezione.

Modulistica cartacea/online:

☐ *Dichiaro di aver preso visione dell'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito www.uniroma3.it/privacy/ e acconsento al trattamento dei miei dati afferenti alle categorie particolari di dati personali ([specificare la tipologia]) per le finalità ivi indicate.*

Modulistica online:

*Cliccando sul pulsante "**[inserire il nome del pulsante come, ad esempio, "Continua", "Invia", etc.]**" dichiaro di aver preso visione dell'Informativa sul trattamento dei dati personali redatta dall'Università degli Studi Roma Tre ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito www.uniroma3.it/privacy/ e acconsento al trattamento dei miei dati afferenti alle categorie particolari di dati personali ([specificare la tipologia]) per le finalità ivi indicate.*

Designazione dell'Incaricato

È incaricato del trattamento qualsiasi persona fisica legittimata, sulla base del ruolo ricoperto nell'organizzazione, a compiere operazioni di trattamento su dati personali. Pertanto sono incaricati del trattamento per conto dell'Università, senza che si renda necessaria alcuna ulteriore formalità, i singoli dipendenti, collaboratori, addetti ai servizi, borsisti cui sono state assegnati compiti specifici nell'ambito delle borse di collaborazione di ateneo, ecc..

Il responsabile interno del trattamento può designare quale incaricato del trattamento un soggetto terzo che debba svolgere operazioni di trattamento di dati personali, ad esclusione dei "dati sensibili", per un periodo limitato di tempo. La designazione avviene in forma scritta e contestualmente sono fornite all'incaricato le istruzioni necessarie a garantire il corretto trattamento in coerenza con gli obiettivi dell'Università e nel rispetto dei principi generali in materia di protezione dei dati personali.

Si ricorda che oltre alle istruzioni di carattere generale è possibile fornire ulteriori indicazioni e istruzioni qualora lo specifico trattamento lo richieda.

OGGETTO: Lettera di designazione quale Incaricato al trattamento dei dati personali

Gentile ***[nome, cognome (nota: trattasi sempre di persona fisica)]***
Nell'ambito del contratto/mansioni assegnate, Le sono fornite di le istruzioni necessarie a garantire il corretto trattamento dei dati personali in coerenza con gli obiettivi dell'Università perseguiti e nel rispetto dei principi generali in materia di protezione dei dati personali.
Durante lo svolgimento delle attività di trattamento dovrà rispettare gli obblighi e attenersi alle istruzioni riportate nel documento "ISTRUZIONI PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI" pubblicato sul sito www.uniroma3.it/privacy/.
Inoltre, dovrà [inserire eventuali istruzioni specifiche per il trattamento eseguito dall'incaricato].
Distinti saluti,
[qualifica e firma]

Nomina a Responsabile del Trattamento

Il responsabile del trattamento è la persona fisica o giuridica, o altro organismo che tratta dati personali per conto del titolare del trattamento. Sono pertanto da considerarsi responsabili del trattamento i fornitori selezionati dall'Università per l'erogazione di servizi che trattano dati personali.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Un fac-simile di contratto è riportato nell'*ALLEGATO 8 - Nomina Responsabile Trattamento*.

Il responsabile del trattamento è sempre un soggetto esterno all'Università.

Clausola per contratti con soggetti titolari autonomi del trattamento

In alcuni casi l'Università autorizza o stipula convenzioni con soggetti terzi al fine di consentire l'instaurazione di un rapporto con il proprio personale e/o studenti/studentesse. In questi casi, solitamente detti soggetti terzi raccolgono direttamente i dati personali dagli interessati e cominciano a trattarli in qualità di autonomi titolari del trattamento.

Per consentire la corretta interpretazione di questo scenario, si forniscono di seguito alcuni esempi:

- l'Università consente ad un fotografo esterno di partecipare ad alcuni eventi tenuti presso l'Università (es. seduta di laurea, inaugurazione dell'anno accademico). Tuttavia, l'Università non riceve i dati raccolti dal fotografo (es. le immagini) né fornisce istruzione alcuna relativamente alle finalità e modalità del trattamento. Pertanto, il fotografo agirà quale autonomo titolare del trattamento ed ogni diritto dovrà essere esercitato dagli interessati direttamente nei suoi confronti;
- l'Università stipula una convenzione con un operatore privato che fornisce servizi a prezzi agevolati per i propri lavoratori e/o studenti e studentesse. Gli utenti si iscrivono autonomamente presso gli uffici dell'operatore o tramite gli strumenti informatici forniti dall'operatore stesso, fornendo i propri dati, che saranno trattati da quest'ultimo per le proprie finalità (es. fornitura del servizio). L'Università non riceve dati personali relativi all'utilizzo del servizio né ne determina le finalità del trattamento. Pertanto, l'operatore privato che fornisce servizi agli utenti agirà quale autonomo titolare del trattamento ed ogni diritto dovrà essere esercitato dagli interessati direttamente nei suoi confronti.

In casi simili a quelli che precedono, l'Università ha interesse a chiarire per iscritto che il terzo soggetto agirà quale autonomo titolare. Inoltre, è raccomandabile l'utilizzo di una clausola di manleva per l'indennizzo degli eventuali danni arrecati dall'Università. Pertanto, si suggerisce di aggiungere al contratto con detti terzi soggetti una clausola del seguente tenore:

Art. XX Autonomi titolari del trattamento

1. Le Parti prendono atto che l'Università degli Studi Roma Tre e [SOGGETTO TERZO] agiranno, ciascuna per proprio conto, quali autonomi titolari del trattamento. [SOGGETTO TERZO] si impegna al rispetto della normativa in materia di trattamento dei dati personali, del Regolamento UE 679/2016 ("GDPR"), del Decreto Legislativo n. 196/2003 (come successivamente emendato dal Decreto Legislativo n. 101/2018) e della normativa nazionale e comunitaria in materia.

2. [SOGGETTO TERZO] accetta di tenere indenne e manlevata l'Università degli Studi Roma Tre in relazione a tutti i costi, le pretese, i danni o le spese sostenute dalla stessa derivanti dall'inadempimento delle obbligazioni previste dal presente articolo, inclusi gli eventuali danni di immagine arrecati, siano essi derivanti da una azione o omissione compiuta dal [SOGGETTO TERZO] direttamente o dai suoi agenti, collaboratori, responsabili, dipendenti o personale in generale.

[SI PREGA DI TENER CONTO CHE LA CLAUSOLA DI CUI AL PUNTO 2 POTREBBE NECESSITARE, A SECONDA DEI CASI, LA SOTTOSCRIZIONE SPECIFICA EX ARTT. 1341-1342 C.C.]

NOMINA DEL RESPONSABILE DEL TRATTAMENTO

È fornito di seguito il fac-simile di contratto per la nomina di un soggetto terzo (persona fisica o giuridica) a responsabile del trattamento. Il contratto è sottoscritto dal titolare del trattamento o dal Dirigente dell'Area Contratti o da altra persona delegata dal titolare del trattamento.

Il fac-simile di contratto potrà essere soggetto ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: *http://www.uniroma3.it/privacy/*.

CONTRATTO SUL TRATTAMENTO DI DATI PERSONALI TRA TITOLARE E RESPONSABILE AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 679/2016

Il presente contratto relativo al trattamento dei dati personali ("Data Processing Agreement" o "Contratto") viene sottoscritto:

TRA

L'Università degli studi Roma Tre, con sede in via Ostiense 159, 00154 Roma, Italia, C.F. e P.I. n. 04400441004 ("Università" o "Titolare");

E

[FORNITORE DELL'UNIVERSITÀ], con sede in via [SEDE LEGALE] C.F. e P.I. n. [CF/PIVA] ("Responsabile" o "Fornitore").

Il Titolare e il Responsabile collettivamente sono indicati come le "Parti" e ciascuno, una "Parte".

PREMESSO CHE

Il [... inserire qualifica, cognome e nome …] RUP del suddetto contratto ha accertato che il Fornitore presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

In base al contratto […inserire i riferimenti al numero/oggetto decontratto…], il Responsabile fornirà all'Università, servizi inerenti alla […inserire la tipologia di servizio (ad es. gestione del patrimonio mobiliare, amministrazione dei servizi per la didattica, servizi di medicina preventiva, ecc) …], che delineano l'oggetto e le finalità del trattamento (i "Servizi").
Il suddetto contratto ha durata sino al […inserire la scadenza del contratto...].

Nell'erogazione dei Servizi, il Responsabile potrà avere accesso o potranno essergli resi disponibili i dati personali relativi [inserire la categoria degli interessati: agli studenti, ai dipendenti, ai fornitori o altra tipologia di interessati] i cui dati sono trattati dall'Università ("Dati Personali").

Con il presente Contratto le Parti intendono regolare gli obblighi del Responsabile con riferimento ai Dati Personali che gli saranno forniti dal Titolare, o a cui avrà accesso, nel corso e al fine dello svolgimento dei Servizi.

Art. 1. Premesse, appendici e definizioni

Le premesse e le appendici al presente Accordo (rispettivamente, le "Premesse" e le "Appendici") costituiscono parte integrante e sostanziale del medesimo.
Ai fini del presente Accordo:

a) "Dati Personali", "Trattamento", "Titolare", "Responsabile" e "Autorità di controllo" avranno il significato attribuito loro nel GDPR.
b) "Sub-responsabile" indica qualsiasi soggetto incaricato dal Responsabile che riceve da quest'ultimo Dati Personali relativi ai Servizi esclusivamente al fine di svolgere attività di Trattamento per conto del Titolare e in conformità alle istruzioni del medesimo Titolare e ai termini del presente Accordo.

c) "Disposizioni Privacy" fanno riferimento, collettivamente, al GDPR, al D.Lgs. 196 del 2003 come modificato dal D.Lgs. 101/2018, nonché delle linee guida emanate dall'Autorità di controllo e dall'European Data Protection Board.

Art. 2. Attività e finalità di trattamento

I dettagli delle attività e finalità di Trattamento dei Dati Personali degli Interessati in esecuzione dei Servizi che saranno svolti dal Responsabile per conto del Titolare ai sensi del presente Accordo sono specificati all'Appendice 1.

Art. 3. Obblighi del responsabile

Il Responsabile concorda e si impegna a:

- trattare i Dati Personali relativi agli Interessati esclusivamente:
  - per conto del Titolare e in conformità alle istruzioni impartite dal Titolare, ivi incluse quelle riportate in Appendice 2;
  - al fine di svolgere i Servizi, o in ogni caso come indicato dal Titolare, in conformità al presente Accordo, e per nessun motivo per finalità proprie;
- non adottare autonome decisioni in ordine alle finalità e alle modalità del Trattamento dei Dati degli Interessati;
- informare tempestivamente il Titolare nel caso in cui, nella esecuzione dei Servizi, le Disposizioni Privacy, o altra normativa, gli imponga di trattare i Dati Personali relativi agli Interessati in maniera non conforme alle istruzioni ricevute dal Titolare stesso;
- adempiere in ogni momento alle Disposizioni Privacy e nello specifico ad adottare tutte le misure richieste ai sensi dell'articolo 32 del GDPR;
- predisporre e mantenere aggiornato un adeguato sistema di protezione e sicurezza dei Dati Personali degli Interessati per evitare la distruzione, la perdita, la modifica, la diffusione di tali dati o l'accesso non autorizzato agli stessi, e controllare periodicamente l'efficacia delle misure di sicurezza adottate, implementando almeno le misure di cui all'Appendice 2;
- trattare tutti i Dati Personali relativi agli Interessati come informazioni confidenziali e non comunicare tali informazioni confidenziali senza il preventivo consenso del Titolare, salvo nel caso in cui sia richiesto dall'autorità giudiziaria, o vi sia un obbligo di divulgazione di tali Dati Personali degli Interessati, ma esclusivamente nei limiti in cui ciò sia strettamente necessario per conformarsi a tale ordine dell'autorità giudiziaria od obbligo;
- adottare misure ragionevoli al fine di assicurare che il proprio personale autorizzato (da intendersi dipendenti, consulenti e collaboratori a vario titolo):
  - sia affidabile;
  - sia a conoscenza della natura confidenziale dei Dati Personali degli Interessati e sia obbligato a mantenere confidenziali e riservati tali Dati Personali degli Interessati;
  - sia a conoscenza e rispetti gli obblighi assunti dal Responsabile in virtù del presente Accordo;
- informare immediatamente il Titolare in merito a:
  - qualsiasi violazione della sicurezza, accesso non autorizzato, appropriazione indebita, perdita, danno o altra compromissione della sicurezza, confidenzialità o integrità dei Dati Personali relativi ai Servizi, sia essa effettiva o potenziale ("Violazione di Sicurezza");

  - qualsiasi reclamo, comunicazione o richiesta ricevuta dal personale del Responsabile o dal Sub-responsabile da parte di un Interessato relativamente ai propri Dati Personali, senza rispondere a tali reclami, comunicazioni o richieste salvo che non sia stato autorizzato dal Titolare;
  - qualsiasi richiesta di informazioni, ispezione, contatto da parte dell'Autorità di controllo relativa ai Dati Personali degli Interessati;
- non appena abbia scoperto una Violazione di Sicurezza e, in ogni caso, non oltre 24 ore dalla scoperta:
  - agire immediatamente per prevenire qualsiasi ulteriore Violazione di Sicurezza;
  - assicurare al Titolare collaborazione ed assistenza piena ed immediata in relazione a qualsiasi comunicazione che il Titolare sia obbligato ad effettuare a seguito di una Violazione di Sicurezza;
- assicurare al Titolare collaborazione ed assistenza piena ed immediata in relazione a qualsiasi reclamo, comunicazione o richiesta per l'esercizio dei diritti da parte di un Interessato, *inter alia*:
  - fornendo al Titolare tutti i dettagli del reclamo, comunicazione o richiesta;
  - se autorizzato dal Titolare, soddisfacendo la richiesta dell'Interessato relativa al Trattamento dei propri Dati Personali nella esecuzione dei Servizi, nei tempi previsti dalla legge e nel rispetto delle istruzioni fornite dal Titolare;
  - fornendo al Titolare qualsiasi Dato Personale che detiene con riferimento all'Interessato, se richiesto in un formato elettronico leggibile e comunemente usato;
  - fornendo al Titolare qualsiasi informazione richiesta dal Titolare con riferimento al Trattamento dei Dati Personali degli Interessati effettuato in esecuzione dei Servizi ai sensi del presente Accordo;
  - correggendo, eliminando o bloccando i Dati Personali degli Interessati;
  - implementando misure tecniche ed organizzative adeguate che garantiscano al Responsabile di adempiere alle obbligazioni di cui al presente articolo;
- assicurare al Titolare collaborazione ed assistenza piena ed immediata in relazione a qualsiasi valutazione relativa all'impatto sulla protezione dei Dati Personali degli Interessati trattati nell'esecuzione dei Servizi o consultazione preventiva che il Titolare sia obbligato ad effettuare con riferimento ai Dati Personali degli Interessati, nonché nell'ambito di investigazioni, richieste di informazioni, ispezioni da parte dell'Autorità di controllo;
- rendere noto al Titolare ogni soggetto che supporti il Responsabile nello svolgimento dell'attività di supervisione del rispetto del presente Accordo;
- mettere a disposizione, su richiesta del Titolare, tutte le informazioni e le prove necessarie a dimostrare che il Responsabile ha adempiuto e stia adempiendo alle sue obbligazioni derivanti dal presente Accordo nonché agli obblighi di cui all'articolo 28 del GDPR;
- mettere a disposizione, su richiesta del Titolare, le proprie strutture per il Trattamento dei Dati Personali degli Interessati al fine di consentire al Titolare di effettuare, direttamente o tramite qualsiasi soggetto indipendente e imparziale selezionato dal Titolare a propria scelta, verifiche e controlli delle attività di Trattamento previste dal presente Accordo;

Art. 4. Sub-responsabile

Il Responsabile concorda e si impegna a:

- fornire immediatamente, su richiesta del Titolare, una copia di qualsiasi accordo concluso con un Sub-responsabile relativo al Trattamento dei Dati Personali degli Interessati effettuato nella fornitura dei Servizi;
- comunicare al Titolare ogni eventuale ricorso ad altri Sub-responsabili affinché il Titolare abbia la possibilità di opporsi alla nomina degli stessi. Il Responsabile deve assicurare che il Sub-responsabile abbia sottoscritto un accordo scritto a norma del diritto dell'Unione o di uno degli Stati Membri che abbia ad oggetto il Trattamento dei Dati Personali degli Interessati effettuato nella fornitura dei Servizi da parte del Responsabile e imponga al Sub-responsabile gli stessi obblighi che sono imposti al Responsabile ai sensi del presente Accordo. Resta inteso che il Responsabile e il Sub-responsabile possono concordare ulteriori aspetti commerciali fintantoché tali accordi non confliggano con il presente Accordo. Qualora il Titolare abbia ragionevoli motivi per opporsi alla nomina, da parte del Responsabile, di un nuovo Sub-responsabile, il Titolare dovrà comunicarlo per iscritto al Responsabile avendo cura di specificare i motivi a fondamento della sua opposizione, entro 30 giorni lavorativi dalla ricezione della suddetta comunicazione. Qualora il Titolare presenti opposizione, il Responsabile si impegnerà a collaborare in buona fede con il Titolare per trovare una proposta accettabile, ragionevole ed alternativa. Qualora il Responsabile non sia in grado di presentare una proposta alternativa entro un termine ragionevole che non dovrà essere superiore a sessanta (60) giorni, il Titolare potrà imporre la cessazione del trattamento, senza che ciò comporti alcuna penale o responsabilità in capo alle Parti, dandone comunicazione scritta al Responsabile entro trenta (30) giorni.

Art. 5. Durata della nomina

Le Parti concordano che in caso di scioglimento, per qualsiasi motivo, di tutti, di alcuni o di uno qualsiasi dei Contratti la nomina di Responsabile decadrà automaticamente e il Responsabile e tutti i Sub-responsabili, su richiesta del Titolare, dovranno restituire al Titolare tutti i Dati Personali degli Interessati (in qualsiasi formato siano detenuti) di cui abbiamo effettuato il Trattamento in esecuzione dei Servizi e, nello specifico, in relazione al o ai Contratti oggetto di scioglimento, nonché le relative copie ovvero cancellare tutti i Dati Personali degli Interessati e distruggere i supporti (cartacei, elettronici, etc.) in cui gli stessi sono contenuti e certificare per iscritto al Titolare di averli, rispettivamente, cancellati e distrutti, a meno che la legge impedisca al Responsabile di restituire, cancellare o distruggere, in tutto o in parte, i Dati Personali degli Interessati e i supporti (cartacei, elettronici, etc.) in cui sono contenuti. In tal caso, il Responsabile si impegna ad assicurare la confidenzialità dei Dati Personali degli Interessati e a restituire e/o cancellare i Dati Personali degli Interessati e le relative copie e distruggere i supporti (cartacei, elettronici, etc.) in cui sono contenuti, come richiesto dal Titolare non appena venga meno l'impedimento di cui sopra.
Le Parti concordano che in caso di prolungamento o rinnovo di alcuni o di uno qualsiasi dei Contratti la nomina di Responsabile si ritiene automaticamente rinnovata sino alla scadenza ultima dei contratti, senza che sia necessario alcun ulteriore atto tra le parti.

Art. 6. Trasferimenti di dati personali verso paesi terzi

Le Parti riconoscono che il Responsabile non tratterà né trasferirà i Dati Personali degli Interessati al di fuori dello Spazio Economico Europeo. Qualora il Responsabile intenda trattare o trasferire i Dati Personali degli Interessati in un paese terzo allo Spazio Economico Europeo (EEA) ("Paese Terzo") per il quale non sussiste una decisione della Commissione UE che riconosce un adeguato livello di protezione dei Dati Personali, sarà

necessario il preventivo consenso scritto del Titolare, e troveranno applicazione le disposizioni di cui ai successivi paragrafi.
In aggiunta alle altre previsioni del presente Accordo, per i trasferimenti di Dati Personali in un Paese Terzo, le Parti dovranno stipulare le clausole contrattuali tipo approvate dall'Unione Europea per i trasferimenti di Dati Personali verso un Paese Terzo riconosciute dalla decisione della Commissione UE del 5 febbraio 2010, notificata con il numero C(2010) 593, ("Clausole Contrattuali Tipo").
Nel caso in cui le Clausole Contrattuali Tipo dovessero essere modificate, sostituite o abrogate dalla Commissione UE o ai sensi delle Disposizioni Privacy, le Parti collaboreranno per concordare una possibile versione aggiornata delle Clausole Contrattuali Tipo o per negoziare un'altra soluzione che consenta il trasferimento dei Dati Personali in conformità con le Disposizioni Privacy.
Le disposizioni di cui al presente articolo esplicano effetti, ove applicabili, anche ai rapporti tra Responsabile ed eventuali Sub-Responsabili.

Art. 7. Responsabilità

Il Responsabile sarà pienamente e direttamente responsabile nei confronti del Titolare di tutti i danni subiti dal Titolare o da terzi a seguito o in conseguenza del Trattamento dei Dati Personali relativo ai Servizi effettuato sia da Responsabile sia da qualsiasi Sub-responsabile da egli nominato, a prescindere che il Titolare si sia opposto o abbia acconsentito a detta nomina.
Fatto salvo il caso di dolo e colpa grave, il Titolare non potrà in alcun modo essere ritenuto responsabile nei confronti del Responsabile e del Sub-responsabile per eventuali danni, di qualsiasi tipo, subiti da questi ultimi in conseguenza della esecuzione del presente Accordo.

Art. 8. Manleva e indennizzo

Il Responsabile accetta di tenere indenne e manlevato il Titolare in relazione a tutti i costi, le pretese, i danni o le spese sostenute dal Titolare, o per le quali il Titolare può essere ritenuto responsabile, derivanti dall'inadempimento delle obbligazioni previste dal presente Accordo, o dalle Disposizioni Privacy, sia da parte del Responsabile o dei suoi agenti, collaboratori, dipendenti o personale in generale sia da parte del Sub-responsabile o dei suoi agenti, dipendenti, collaboratori o personale in generale.

Art. 9. Costi

Ogni Parte adempirà alle rispettive obbligazioni previste dal presente Accordo a proprie spese.

Art. 10. Miscellanea

In caso di contrasto tra le disposizioni del presente Accordo e le disposizioni di qualsiasi altro accordo concluso tra le Parti, le disposizioni del presente Accordo prevarranno con riferimento al Trattamento dei Dati Personali effettuato in conseguenza della fornitura dei Servizi.
Nel caso in cui una o più disposizioni del presente Accordo fossero o divenissero illegittime, invalide o inefficaci sotto qualsiasi aspetto, tale illegittimità, invalidità o inefficacia non renderà, illegittime, invalide o inefficaci le rimanenti disposizioni del presente Accordo. Nei limiti del possibile, le disposizioni ritenute illegittime, invalide o inefficaci saranno interpretate o sostituite in maniera tale da riflettere il più fedelmente possibile l'intento contrattuale delle Parti.
Qualsiasi modifica del presente Accordo dovrà essere effettuata per iscritto e sottoscritta da un firmatario debitamente autorizzato delle Parti.

Art. 11. Legge applicabile e foro competente

Il presente Accordo è disciplinato e deve essere interpretato ai sensi della legge italiana.
Il foro esclusivamente competente per qualsiasi controversia tra il Titolare e il Responsabile che non possa essere risolta in modo amichevole e che riguardi l'interpretazione, l'adempimento, la violazione, la risoluzione o l'esecuzione del presente Accordo, è quello di Roma.

Per il Titolare	Per il Responsabile
_____	_____
Nome e cognome	Nome e cognome
_____	_____
Ruolo	Ruolo
_____	_____
Luogo/Data	Luogo/Data

Ai sensi e per gli effetti di cui agli art. 1341 e 1342 del Codice Civile, il Responsabile dichiara di aver letto, compreso e accettato espressamente le seguenti clausole: Art. 4 Sub-responsabile Art. 6 Trasferimenti di dati personali verso paesi terzi, Art. 7 Responsabilità, Art. 8 Manleva e indennizzo, Art. 11 Legge applicabile e foro competente.

Per il Responsabile

_____
Nome e cognome

_____
Ruolo

_____
Luogo/Data

APPENDICE 1
DETTAGLI DELLE ATTIVITÀ DI TRATTAMENTO

Interessati

I Dati Personali oggetto di Trattamento in esecuzione dei Servizi riguardano

- [inserire: ad es., studenti, dipendenti, fornitori, etc.]

Categorie di Dati Personali

I Dati Personali degli Interessati riguardano le seguenti categorie di dati [inserire maggiori informazioni, quali, ad esempio]:

- "Dati identificativi" (nome, cognome, codice fiscale e altri dati degli Interessati);
- "Dati di contatto" (numero telefonico, indirizzo di spedizione, email, etc.);
- Ecc.

Attività di Trattamento

Nell'esecuzione dei Servizi da parte del Responsabile, i Dati Personali relativi agli Interessati saranno soggetti alle seguenti attività di Trattamento da parte del Responsabile: [specificare le attività che vengono svolte quali ad esempio: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto, interconnessione, limitazione, cancellazione, distruzione].

Finalità del Trattamento e base giuridica

Nell'esecuzione dei Servizi da parte del Responsabile, i Dati Personali relativi agli Interessati saranno trattati per le seguenti finalità [specificare le finalità e le basi giuridiche del trattamento, ad esempio]:

- erogazione dei servizi didattici e di segreteria studenti;
- organizzazione e svolgimento di iniziative volte all'orientamento in ingresso, in itinere ed in uscita;
- organizzazione di test di valutazione o ammissione a qualunque corso di;
- organizzazione delle attività di collaborazione e dei tirocini extracurriculari;
- erogazione dei servizi informatici e accesso ai laboratori e ad altre strutture protette;
- erogazione dei servizi di e-learning;
- erogazione di servizi di tutorato, assistenza, inclusione sociale;
- sondaggi condotti anonimamente e su base aggregata;
- ecc.

Durata del Trattamento

I Dati Personali degli Interessati saranno trattati dal Responsabile per tutta la durata dei Servizi e, al termine degli stessi, restituiti al Titolare o cancellati nel rispetto delle previsioni del presente Accordo.

APPENDICE 2
MISURE TECNICHE E ORGANIZZATIVE DI SICUREZZA
Descrizione delle misure tecniche e organizzative di sicurezza implementate e mantenute dal Responsabile

Il Responsabile si impegna a garantire che il proprio personale autorizzato e i propri Sub-responsabili osservino, in ogni momento, gli obblighi contenuti nelle *Istruzioni per il corretto trattamento dei dati personali* allegate al *Regolamento di Ateneo in materia di protezione dei dati personali* nonché le misure di cui al documento [inserire eventuale documentazione aggiuntiva o rimuovere il testo da "nonché le misure…"].

In ogni caso, il Responsabile si impegna ad adottare le seguenti misure tecniche e organizzative minime:

- I Dati Personali degli Interessati devono essere, ove possibile o necessario ai sensi della normativa, cifrati o pseudonomizzati, a seconda dei casi. Opportune salvaguardie devono essere adottate sia per i formati digitali che fisici.
- Prodotti contro i malware e antivirus devono essere installati, operanti e aggiornati su ogni hardware ivi inclusi, a titolo esemplificativo e non esaustivo, computer, laptop, server, router, dispositivi mobili.
- La conservazione e il Trattamento dei Dati Personali degli Interessati in dispositivi portatili o al di fuori dei locali del Responsabile, saranno soggetti al rispetto di specifiche policy e procedure e, in ogni caso, garantiranno il livello di sicurezza che si renderà necessario in relazione al tipo di file trattato.
- Qualora i supporti e i documenti contenenti Dati Personali degli Interessati, siano portati fuori dai locali sotto il controllo del Responsabile, tale circostanza dovrà essere disciplinata da specifiche procedure. Le necessarie misure di sicurezza saranno implementate durante il trasferimento dei supporti e della documentazione, al fine di evitare furti, perdite o accessi non autorizzati alle informazioni durante il trasporto.
- I sistemi di archiviazione temporanea o le copie di documenti creati esclusivamente per l'esecuzione di attività temporanee o ausiliarie devono rispettare un livello di sicurezza adeguato e devono essere cancellati o distrutti una volta che non siano più necessari per le finalità per le quali sono stati creati.
- Le procedure di back-up devono essere documentate. Le copie di backup complete devono essere conservate.
- In tema di distaster recovery, devono essere implementate procedure per ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidenti fisici o tecnici. Ciò include anche la predisposizione di un piano di disaster recovery per i sistemi attraverso i quali sono trattati Dati Personali degli Interessati.
- Saranno implementati controlli degli accessi sia digitali che fisici. Le misure di controllo degli accessi dovranno essere documentate mediante policy scritte e procedure interne. Inoltre, il Responsabile adotterà policy e procedure rispetto a:
    - procedure di autenticazione multi fattore;
    - limitazione dell'accesso ai dati unicamente a persone che ne abbiano necessità per poter adempiere ai propri obblighi.
- Il Responsabile assicura che le persone autorizzate al Trattamento abbiano accesso solo ai dati necessari per compiere le proprie mansioni. Le funzioni e gli obblighi di ogni persona autorizzata con accesso ai Dati Personali degli Interessati e ai sistemi informativi saranno chiaramente definiti e documentati.

- Il Responsabile deve garantire l'esistenza di un elenco aggiornato delle persone autorizzate al Trattamento dei Dati Personali degli Interessati e degli accessi autorizzati per ciascuno di essi.
- Il Responsabile stabilirà meccanismi per evitare che un soggetto possa accedere a Dati Personali degli Interessati in modo diverso rispetto alle modalità con le quali tale soggetto è autorizzato ad accedere agli stessi.
- Quando il meccanismo di autenticazione si basa sull'esistenza di password, sarà implementata dal Responsabile una procedura per l'assegnazione, la distribuzione e la memorizzazione di tali password al fine di garantirne la riservatezza e l'integrità. Analogamente, le password saranno sostituite dal Responsabile con cadenza regolare, che comunque non potrà superare sei mesi, e saranno conservate in modo tale da renderle inintelligibili durante il periodo di validità.
- I luoghi dove sono conservati i Dati Personali degli Interessati saranno soggetti a restrizioni e verrà tenuto un inventario di tali luoghi. L'accesso a luoghi dove sono conservati i dei Dati Personali degli Interessati al di fuori delle relative ore di lavoro sarà registrato dal Responsabile, con la indicazione di: ora entrata, ora uscita, persona che accede al luogo.

PERIODO DI CONSERVAZIONE DEI DATI

Linee guida per la conservazione di talune tipologie di dati e documentazione.

La presente guida potrà essere soggetta ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/

Tipologia di dati e documentazione[1]	**Inizio del periodo di conservazione cui segue la cancellazione**[2]	**Periodo di conservazione**[3]
Caselle e-mail degli studenti e relativi messaggi in essi contenuti	Data di conseguimento del titolo	5 anni
Dati biometrici (es. impronta, retina, grafia, ecc.) di accesso agli edifici	Data di acquisizione	7 giorni
Dati di videosorveglianza e/o immagini registrate tramite CCTV	Data della registrazione	7 giorni
Certificati idoneità fisica per attività sportiva anche dilettantistica	Termine dell'anno accademico in cui si è svolta l'attività sportiva	1 anno
Videoregistrazioni su piattaforme e-learning delle lezioni relative ad una attività formativa	Termine dell'anno accademico in cui è stata erogata l'attività formativa	3 anni
Valutazioni di esami pubblicati sul web	Data di pubblicazione	3 mesi
Risultati di procedure di selezione semplificate	Data di pubblicazione	6 mesi (salvo diverse disposizioni di legge)

[1] Descrizione del tipo di documento e delle categorie di dati personali che lo caratterizzano.
[2] L'evento a partire dal quale si dà inizio del periodo di conservazione (ad esempio la data di conseguimento del titolo). Al termine del periodo di conservazione si procede alla cancellazione dei documenti/dati.
[3] Termine massimo di conservazione dei documenti/dati. Il termine non eccede quanto necessario riguardo agli scopi per i quali i dati personali sono stati raccolti, considerando anche eventuali obblighi di legge.

VALUTAZIONE D'IMPATTO

Scheda di valutazione d'impatto sulla protezione dei dati personali da compilare a cura del responsabile interno del trattamento.

La presente scheda potrà essere soggetta ad eventuali aggiornamenti. La versione aggiornata è sempre disponibile all'indirizzo: http://www.uniroma3.it/privacy/

Sommario

AMBITO DEL TRATTAMENTO

(Di seguito sono individuati gli elementi essenziali del trattamento.)

Titolo del trattamento

(Inserire il titolo del trattamento che si intende proporre)

Descrizione del trattamento

(Ove possibile non superare i 4.000 caratteri, spazi inclusi)

Finalità del trattamento

(Ove possibile non superare i 4.000 caratteri, spazi inclusi)

Operazioni di trattamento compiute

(Ove possibile non superare i 4.000 caratteri, spazi)

SOGGETTI COINVOLTI

Eventuale Co-Titolare del trattamento

(Ove previsto)

Eventuale Responsabile del trattamento

(Ove previsto)

Strutture coinvolte

(Indicare gli Uffici e/o dipartimenti coinvolti, inclusi i responsabili interni e le categorie di incaricati)

VALUTAZIONE

(Per ognuno dei seguenti punti dovranno indicarsi, da un lato, gli aspetti concernenti il possibile impatto sulla privacy degli interessati (probabilità e gravità dei rischi, requisiti di conformità, etc.), dall'altro, le misure messe in atto alla luce dei rischi individuati (garanzie e meccanismi di protezione dei dati, misure di sicurezza, procedure per il trattamento, istruzioni agli incaricati specifiche etc.). Di seguito a ciascun elemento di valutazione sono indicati in corsivo, a mero scopo esemplificativo e non esaustivo, alcuni quesiti di guida alla compilazione dei rispettivi campi.)

Trasparenza degli interessati

(Come vengono portati a conoscenza dell'esistenza del trattamento gli interessati? L'interessato si aspetta che il titolare del trattamento realizzi questo tipo di trattamento? È necessario fornire una informativa visiva o semplificata di qualche tipo?)

Rischi: …

Contromisure: …

Individuazione della base giuridica

(Come è stata individuata la base giuridica? Quali conseguenze, anche negative, comporterebbe l'adozione di una base giuridica piuttosto che un'altra?)

Rischi: …

Rimedi: …

Rispetto del principio di finalità

(Come sarà assicurata la corrispondenza del trattamento rispetto alle finalità perseguite? È possibile che i dati siano trattati per finalità diverse? È possibile che dal presente trattamento derivino trattamenti ulteriori per finalità difformi?)

Rischi: …

Contromisure: …

Principio di accuratezza ed esattezza dei dati

(Come viene assicurata l'accuratezza, l'esattezza e l'aggiornamento dei dati? Quali meccanismi saranno messi in atto, manuali o non, al fine di garantire tali principi? Quali sono i rischi derivanti dalla mancata accuratezza dei dati?)

Rischi: …

Contromisure: …

Minimizzazione dei dati

(Quali conseguenze potrebbe portare un utilizzo eccessivo dei dati o l'esistenza di dati eccedenti? È un rischio plausibile nel trattamento delineato in premesse? Come viene assicurato che i dati trattati siano esclusivamente quelli necessari per il trattamento?)

Rischi: …

Contromisure: …

Periodo di conservazione dei dati

(Quali conseguenze potrebbe portare una eccessiva conservazione dei dati nell'ambito del trattamento descritto in premesse? Come è garantita l'uniformità rispetto ad altri periodi di conservazione individuati nell'Ateneo? Se e quali procedura saranno messe in atto per assicurare il rispetto del periodo di conservazione dei dati individuato?)

Rischi: …

Contromisure: …

Esercizio dei diritti da parte degli interessati

(Quali diritti potranno essere esercitati dagli interessati, in quanto applicabili al caso concreto? Quali sono i possibili limiti al soddisfacimento dei diritti degli interessati nell'ambito di questo trattamento? Saranno previsti strumenti automatizzati per l'esercizio dei diritti da parte degli interessati?)

Rischi: …

Contromisure: …

Sicurezza della conservazione dei dati

(I dati saranno conservati in formato cartaceo o elettronico? Se in formato cartaceo, dove saranno conservati i documenti? Se in formato elettronico, quali sono le misure di sicurezza da implementare?)

Rischi: …

Contromisure: …

Rapporti con soggetti terzi che trattano i dati (es. fornitori, incaricati del trattamento estranei all'Ateneo, etc.).

(Quali potrebbero essere i rischi derivanti dal coinvolgimento di soggetti terzi all'Ateneo? Quali misura sono adottate al fine di minimizzare tali rischi? Sarà facile individuare, di volta in volta e in corso di trattamento, i soggetti coinvolti?)

Rischi: …

Contromisure: …

Trasferimenti di dati al di fuori del territorio dell'Unione Europea

(Quali sono le misure adottate al fine di garantire la protezione dei dati degli interessati nell'ambito dei trasferimenti di dati al di fuori del territorio dell'Unione Europea? Per quali motivi è stato scelto uno strumento giuridico piuttosto che un altro per porre in essere detto trasferimento? È stata considerata la possibilità che i responsabili del trattamento pongano in essere trasferimenti al di fuori dell'Unione Europea?)

Rischi: …

Contromisure: …

INDIVIDUAZIONE DEI RISCHI PER GLI INTERESSATI

(Quali sono i rischi che potrebbero derivare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, con riferimento alla specifica tipologia di dati trattati e di categoria di interessati?)

Data _____

Firma del Dirigente/Direttore di Dipartimento/Centro, Presidente della Scuola

_____

PARERE DEL RESPONSABILE PER LA PROTEZIONE DEI DATI (DPO)

(Sintesi del parere espresso dal DPO con l'indicazione della necessità di sottoporre la valutazione di impatto ad un consesso composto dal Rettore, dal Direttore Generale, da un membro del Consiglio di Amministrazione individuato secondo le competenze specifiche del caso, dal Dirigente competente e dal DPO)

Data _____ *Firma del DPO _____*

OSSERVAZIONI

(Eventuali osservazioni formulate da soggetti rappresentativi degli interessati, ad es. rappresentanti dei lavoratori, rappresentanti degli studenti, associazioni di categoria, etc.)

DETERMINAZIONI DEL TITOLARE

Ad esito della valutazione di impatto, del bilanciamento degli interessi in gioco, e dell'eventuale parere espresso dal consesso composto dal Rettore, dal Direttore Generale, da un membro del Consiglio di Amministrazione individuato secondo le competenze specifiche del caso, dal Dirigente competente e, considerate le osservazioni formulate dal DPO, si ritiene che il trattamento comporti:

- ☐ *un rischio elevato – è necessario provvedere con la consultazione del Garante per la protezione dei dati personali;*
- ☐ *nessun rischio rilevante – si può procedere con il trattamento.*

Data _____ *Firma del Titolare del Trattamento _____*