



L'Università Europea di Roma, con sede legale a Roma, via degli Aldobrandeschi n. 190, in qualità di Titolare del Trattamento (di seguito anche "Università" o "Titolare") avendoLa autorizzata al trattamento dei dati ai sensi dell'art. 29 del Regolamento (UE) n. 2016/679, recante il "Regolamento Generale sulla Protezione dei Dati personali" (di seguito anche "RGPD"), con la presente intende fornirLe le istruzioni, che costituiscono parte integrante del Regolamento sul trattamento dei dati personali svolto dall'Università (di seguito anche "Regolamento") alle quali Lei è tenuto ad attenersi pedissequamente nel trattare i dati di cui l'Università è titolare.

In caso di dubbi sull'interpretazione del Regolamento o delle presenti istruzioni può rivolgersi al Responsabile della Protezione dei dati personali ("DPO"), l'avv. Elena Maggio, che può essere contattata al seguente indirizzo e-mail dpo.emaggio@unier.it o chiamando al numero 333.2160001.

1. Ambito di applicazione del RGPD e del Regolamento

Sono soggetti alle prescrizioni del RGPD tutti i soggetti stabiliti nell'Unione Europea e i soggetti che, ancorché non stabiliti, offrono beni o servizi, anche gratuitamente, a soggetti che si trovano nell'Unione, siano essi cittadini o meno di uno degli Stati membri. Quindi, ad esempio, Lei è tenuto al rispetto delle presenti istruzioni anche quando tratta dati di studenti non europei.

Il Regolamento non si applica esclusivamente ai trattamenti di dati personali effettuati da persone fisiche nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale, quali la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività.

Ancorché il Regolamento tuteli espressamente i soli dati delle persone fisiche deve ricordarsi che ai sensi del Provvedimento del 20 settembre 2012 del Garante per la protezione dei dati personali non possono essere inviati messaggi di posta elettronica a persone giuridiche senza il previo consenso di questo ultime, salva l'ipotesi in cui la persona giuridica sia o sia stata in passato già cliente.

Il Regolamento è volto a definire l'assetto organizzativo e le procedure per il trattamento dei dati personali svolto da parte dell'Università che assicuri il rispetto dei diritti, delle libertà fondamentali, nonché della dignità di quanti hanno rapporti con l'Università, con particolare riferimento alla riservatezza ed all'identità personale degli interessati, siano essi interni o esterni alla stessa.

2. Come trattare i dati

Nello svolgere i trattamenti che Le vengono richiesti dall'Università, è tenuto ad applicare le previsioni di cui al Regolamento e i seguenti principi generali di cui all'art. 5 del RGPD:

- liceità (rispetto delle norme), correttezza (rispetto delle reciproche esigenze dell'interessato e del titolare) e trasparenza (verso l'interessato affinché possa legittimamente fondare il proprio consenso) del trattamento dei dati personali;
- integrità e riservatezza: i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, evitando inutili duplicazioni dei dati che ne aumentano il rischio di perdita;
- minimizzazione: i dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;



- esattezza: i dati personali raccolti devono essere esatti e, se necessario, aggiornati anche prevedendo misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- limitazione delle finalità: i dati personali devono essere raccolti esclusivamente per le finalità determinate dall'Università e indicate nell'informativa che Lei è tenuto a somministrare nel momento in cui raccoglie dati;
- limitazione della conservazione: i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per 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).

3. Misure di sicurezza adeguate al trattamento

L'Università definisce le misure di sicurezza adeguate alle tipologie di trattamenti posti in essere in qualità di titolare. In generale, si ricorda che Le è fatto divieto di:

- a) comunicare i dati personali il cui trattamento Le viene affidato a colleghi, collaboratori o fornitori dell'Università, a meno di espressa richiesta e/o autorizzazione da parte dell'Università;
- b) comunicare i dati personali il cui trattamento Le viene affidato a soggetti terzi che non siano stati preventivamente individuati dall'Università.

Le misure sono distinte a seconda delle modalità con cui il trattamento è realizzato:

- 1) trattamenti cartacei;
- 2) trattamenti con l'ausilio di strumenti elettronici.

3.1. Misure di sicurezza in caso di trattamenti cartacei

Qualora Lei tratti dei dati in modalità cartacea nei locali dell'Università è tenuto a:

- a) custodire i documenti contenenti dati personali in modo da evitare che terzi possano accedervi, non lasciando tali documenti incustoditi all'interno dell'ufficio o sulla postazione messa a Sua disposizione e evitando di portarli fuori dalla sede dell'Università tali documenti;
- b) non comunicare i dati personali il cui trattamento Le viene affidato a colleghi, collaboratori o fornitori dell'Università, salvo espressa richiesta del Suo superiore o designato;
- c) non comunicare in alcun caso i dati personali il cui trattamento Le viene affidato a soggetti terzi che non siano stati preventivamente individuati dall'Università;
- d) non copiare e/o digitalizzare i documenti, salvo espressa richiesta del Suo superiore o designato;
- e) distruggere, ove Le venga espressamente richiesto, i documenti recanti i dati personali.

Qualora Lei tratti dei dati in modalità cartacea per ragioni di servizio al di fuori dei locali dell'Università è tenuto a:

- a) custodire i documenti contenenti dati personali in modo da evitare che terzi possano accedervi, ad esempio non lasciando tali documenti incustoditi in locali pubblici o in ambienti, anche domestici, ove possano accedervi persone estranee al nucleo familiare di appartenenza;



- b) non comunicare i dati personali il cui trattamento Le viene affidato a colleghi, collaboratori o fornitori dell'Università, salvo espressa richiesta del Suo superiore o designato;
- c) prestare attenzione nel corso di comunicazioni telefoniche a che persone estranee possano indirettamente acquisire dati personali;
- d) non comunicare in alcun caso i dati personali il cui trattamento Le viene affidato a soggetti terzi che non siano stati preventivamente individuati dall'Università;
- d) non copiare e/o digitalizzare i documenti, salvo espressa richiesta del Suo superiore o designato;
- e) distruggere ogni copia di documenti, creata nei limiti di cui alla lett. e), non appena la conservazione del documento non sia più necessaria;
- f) riportare tempestivamente i documenti originali che dovesse aver portato fuori dai locali dell'Università negli uffici provvedendo all'archiviazione e conservazione degli stessi, garantendone nelle more idonea e adeguata conservazione.

3.2. Misure di sicurezza in caso di trattamenti elettronici

Qualora Lei tratti dei dati nei locali dell'Università con l'ausilio di strumenti elettronici è tenuto a:

- a) utilizzare esclusivamente i sistemi informatici, i software e gli strumenti gestionali messi a disposizione dall'Università;
- b) non accedere a sistemi informatici, software e strumenti gestionali con terminali diversi da quelli messi a Sua disposizione dall'Università;
- c) custodire con cura e diligenza le Sue credenziali per l'utilizzo dei sistemi informatici, software e strumenti gestionali messi a disposizione dall'Università;
- d) non cedere o divulgare le Sue credenziali per l'utilizzo dei sistemi informatici, software e strumenti gestionali messi a disposizione dall'Università;
- e) aggiornare almeno ogni tre mesi la password di accesso ai sistemi informatici, software e strumenti gestionali, secondo gli standard definiti dall'Università;
- f) non utilizzare sistemi di memorizzazione automatica delle credenziali di accesso, specie nell'ipotesi in cui utilizzi un terminale di Sua proprietà;
- g) non lasciare incustodito e/o liberamente accessibile, anche se all'interno dei locali dell'Università, il terminale tramite il quale sta svolgendo il trattamento;
- h) non modificare le impostazioni di sicurezza del Suo terminale, non installare software, salvo espressa deroga, e non utilizzare dispositivi (quali pen drive o similari) di cui si sia assolutamente certi della integrità e assenza di virus;
- i) non creare copie di lavoro, cartacee o digitali, backup e similari dei dati personali di cui Le viene affidato il trattamento al di fuori dei sistemi informatici, software e strumenti gestionali;
- j) qualora il Suo superiore o designato Le chieda di realizzare una copia analogica (stampa) di un documento informatico è tenuto a non lasciare incustodito il documento presso la stampante condivisa e a distruggerla non appena la conservazione della copia non sia più necessaria.

Qualora Lei tratti dei dati per ragioni di servizio al di fuori dei locali dell'Università con l'ausilio di strumenti elettronici è tenuto a:



- a) utilizzare esclusivamente i sistemi informatici, i software e gli strumenti gestionali messi a disposizione dall'Università, salvo deroga che sarà concessa previa verifica della sicurezza del terminale che intende impiegare;
- b) non accedere a sistemi informatici, software e strumenti gestionali con terminali diversi da quelli messi a Sua disposizione dall'Università;
- c) non accedere a sistemi informatici, software e strumenti gestionali con connessioni internet (wireless e non) non sicure o aperte che non richiedono l'identificazione dell'utente;
- d) custodire con cura e diligenza le Sue credenziali per l'utilizzo dei sistemi informatici, software e strumenti gestionali messi a disposizione dall'Università;
- e) non cedere o divulgare le Sue credenziali per l'utilizzo dei sistemi informatici, software e strumenti gestionali messi a disposizione dall'Università;
- f) aggiornare almeno ogni tre mesi la password di accesso ai sistemi informatici, software e strumenti gestionali, secondo gli standard definiti dall'Università;
- g) non utilizzare sistemi di memorizzazione automatica delle credenziali di accesso, specie nell'ipotesi in cui utilizzi un terminale di Sua proprietà;
- h) non lasciare incustodito e/o liberamente accessibile il terminale tramite il quale sta svolgendo il trattamento, specie se si trova in luoghi aperti al pubblico;
- i) non modificare le impostazioni di sicurezza del Suo terminale, non installare software, salvo espressa deroga, e non utilizzare dispositivi (quali pen drive o similari) di cui si sia assolutamente certi della integrità e assenza di virus;
- j) non creare copie di lavoro, cartacee o digitali, backup e similari dei dati personali di cui Le viene affidato il trattamento al di fuori dei sistemi informatici, software e strumenti gestionali;
- k) qualora il Suo superiore o designato Le chieda di realizzare una copia analogica (stampa) di un documento informatico è tenuto a distruggerla non appena la conservazione della copia non sia più necessaria.

4. Obbligo di aggiornamento

Lei ha l'obbligo di partecipare con la dovuta diligenza alle iniziative formative promosse dal DPO ed a studiare il materiale formativo messo a sua disposizione, aggiornandosi periodicamente sulle *best practice* in materia di trattamento dei dati personali, anche tramite lo studio del materiale informativo messo a disposizione dall'Università.

5. Sanzioni

Il mancato rispetto da parte delle istruzioni impartite potrà comportare l'avvio di un procedimento disciplinare e, nei casi più gravi, la risoluzione di diritto del contratto di lavoro, anche nell'ipotesi in cui da ciò non discenda l'avvio di un procedimento sanzionatorio da parte del Garante Privacy o non consegua la richiesta di danni da parte di un interessato.

Lei è tenuto a tenere indenne, in caso di dolo o colpa grave, l'Università dal pagamento di sanzioni e/o refusione per eventuali danni cagionati a terzi che siano conseguenza del trattamento difforme rispetto alle istruzioni impartite.