



ISTRUZIONI PER GLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Nelle more dell'aggiornamento delle "norme comportamentali" e del rilascio di ulteriori documenti e regolamenti interni, ciascun autorizzato al trattamento è tenuto al rispetto della normativa in materia e delle seguenti istruzioni.

DEFINIZIONI

- **dato personale:** qualsiasi informazione riguardante una **persona fisica** identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **violazione dei dati personali:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **categorie particolari di dati personali** (art. 9 REG. (UE) 2016/679): dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale, i dati genetici, i dati biometrici e i dati relativi alla salute
- **dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **dati biometrici:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **dati giudiziari:** i dati relativi a condanne penali e reati: si tratta dei dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
- **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; (...)

- **Delegati del Titolare** i soggetti **interni** dell'ateneo individuati dal Titolare con Decreto Rettoriale Rep 921 prot. 27064 del 12/03/2019 ed a cui sono affidati specifici compiti (Dirigenti, Direttori Dipartimento etc...);
- **Responsabile** (esterno) **del trattamento** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. (...)
- **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;
- **Data Protection Officer/Responsabile per la protezione dei dati** figura specializzata nel supporto al Titolare del trattamento, obbligatoria negli enti pubblici;
- **Amministratore di sistema**: la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- **Autorizzati al trattamento**: le persone fisiche che hanno accesso ai dati personali e trattano gli stessi mediante l'autorizzazione e le istruzioni ricevute dal titolare del trattamento e suoi delegati, tra cui i docenti, il personale tecnico-amministrativo, i tesisti, i tirocinanti, gli stagisti, studenti delle 150 ore ed ogni altra figura a questi affini;
- **Interessato al trattamento**: la persona fisica cui si riferiscono i dati personali;

PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

Il trattamento dei dati da parte degli autorizzati dovrà avvenire nel rispetto dei principi del Reg. (UE) 2016/679, del Decreto Legislativo 30 giugno 2003, n.196 ("Codice privacy") e se m.i., della normativa connessa e delle ulteriori disposizioni impartite dal Titolare.

Pertanto i dati personali, ai sensi dall'articolo 5 del REG. (UE) 2016/679 dovranno essere:

- a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**liceità, correttezza e trasparenza**);
- b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (**limitazione della finalità**);
- c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**minimizzazione dei dati**);
- d. 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 (**esattezza**);
- e. 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 all'articolo 89, paragrafo 1, (...) (**limitazione della conservazione**);
- f. 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 accidentali (**integrità e riservatezza**).

Ogni soggetto che opera nell'Università è chiamato, nello svolgimento delle proprie funzioni, a trattare dati personali, rispetto ai quali dovrà attenersi anche ai seguenti primi principi generali di azione:

- verificare sempre la natura del dato personale per distinguere i dati personali comuni da quelli particolari (sensibili) e giudiziari al fine di riservare a queste due ultime specifiche categorie le particolari autorizzazioni e cautele di trattamento e custodia che richiedono;
- mantenere in ogni caso la massima riservatezza sui dati oggetto del trattamento, il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante l'attività prestata;
- non utilizzare, comunicare o diffondere (anche solo rendendo possibile la loro consultazione) i dati se non previa autorizzazione del Titolare del trattamento o suoi delegati;
- in generale, prestare la più ampia e completa collaborazione al Titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- conservare i dati nella forma che permette l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
- operare esclusivamente su dati cui si è autorizzati all'accesso, nel rispetto dei principi di pertinenza ed essenzialità dei dati trattati;
- razionalizzare gli archivi;
- nelle relazioni con enti terzi, operare la comunicazione dei dati solo se necessaria ed autorizzata;
- monitorare l'insorgenza di nuovi rischi di sicurezza e comunicarli al Titolare;
- non comunicare a terzi o diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi;
- segnalare con tempestività al Delegato o al proprio responsabile di ufficio/superiore eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante privacy ed ai soggetti interessati.

GESTIONE DEI CODICI DI IDENTIFICAZIONE E PASSWORD

- custodire con la massima cura e non condividere tra più utenti i codici di identificazione personale (username/user-id) e le password.
- User-id e password di accesso alle postazioni di lavoro (pc), server, strumenti/applicativi informatici con cui vengono trattati e/o custoditi i dati sono riservate, personali e non cedibili;
- impostare la password con una lunghezza di almeno 8 caratteri, di cui almeno un carattere speciale ed una lettera maiuscola, senza riferimenti personali o informazioni facilmente deducibili, quali il proprio nome, il nome dei familiari, la data di nascita, il proprio codice fiscale etc...;
- non lasciare codici identificativi/password incustoditi su fogli, agendine, post-it, affinché non risultino esposte facilmente all'accesso di terzi;
- le password devono essere sostituite, a cura del singolo autorizzato:
 - almeno ogni sei mesi, salvo il caso di perdita della sicurezza della stessa;
 - almeno ogni 3 mesi in caso di trattamento di dati particolari (sensibili/giudiziari) salvo il caso di perdita della sicurezza della stessa;
 - in caso di modifica della password non riutilizzare le precedenti 5;
- utilizzare una password differente per ogni servizio/applicativo usato.
- Nel caso in cui una password perda di segretezza, l'autorizzato deve provvedere alla sua immediata sostituzione. Quando questo non risulti possibile, l'autorizzato deve comunicare tale circostanza al competente Amministratore di Sistema.

GESTIONE DEI LOCALI E DELLE POSTAZIONI DI LAVORO

- verificare che l'accesso agli archivi cartacei contenenti dati personali sia limitato ai soli soggetti autorizzati, in quanto lo stesso è consentito esclusivamente al fine di estrarre i soli dati necessari allo svolgimento dei compiti istituzionali loro assegnati;
- i documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento, non rimanere incustoditi su scrivanie o postazioni di lavoro e riposti negli archivi a fine giornata;
- verificare sempre, in caso di allontanamento anche temporaneo dalla postazione di lavoro, che non sia possibile per altri accedere ai dati personali dei quali è in corso il trattamento, qualunque sia il tipo di supporto su cui sono contenuti i dati, ad esempio disconnettendo i dispositivi che consentono di accedere ai dati stessi, bloccando il pc affinché sia possibile riaccedervi solo tramite password, riponendo sotto chiave i documenti o i fascicoli che li contengono;
- avere cura di prelevare i documenti cartacei dagli archivi, nel rispetto delle regole previste nel Manuale di gestione documentale e comunque per il tempo strettamente necessario allo svolgimento delle mansioni e di custodirli durante l'uso in maniera che ne sia garantita la sicurezza;
- custodire atti e documenti contenenti dati personali particolari/sensibili o giudiziari in armadiature munite di serratura e controllare che a tali atti e documenti non possano assolutamente accedere persone prive di specifica autorizzazione e nei limiti della stessa;
- restituire immediatamente al termine delle operazioni affidate atti e documenti contenenti dati sensibili o giudiziari;
- osservare scrupolosamente, per quanto concerne l'utilizzo degli strumenti informatici, le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica e logica adottate dall'Università;
- la mera abilitazione tecnica all'accesso a banche dati non equivale a un generale autorizzazione alla consultazione o estrazione di tutti i dati contenuti; tali attività devono comunque essere limitate (nei modi, nelle tipologie e nei tempi) alle specifiche funzioni di servizio di ciascun autorizzato;
- accertarsi sempre dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita;
- non comunicare dati personali a mezzo email, telefono, fax od altra modalità senza specifica autorizzazione e identificazione del richiedente legittimato a riceverli;
- avere cura di non salvare, caricare, elaborare e trattare in generale dati personali non afferenti alla sfera istituzionale dei quali si è in possesso anche in ragione di attività professionali esterne all'Ateneo.

Il Direttore Generale

(Dott. Cristiano Nicoletti)

