UNIVERSITÀ DEGLI STUDI DI MILANO

Istruzioni generali per il trattamento dei dati personali, ai sensi dell'Articolo 32, comma 4[1] del Regolamento Europeo per la Protezione dei Dati (GDPR)

L'Università degli Studi di Milano, in qualità di titolare del trattamento dei dati personali, dell'Ateneo, dispone che chiunque abbia accesso a tali dati, li consulti, li archivi, li diffonda, li modifichi, li raccolga o, comunque, effettui qualsiasi operazione su informazioni, sia in formato elettronico che cartaceo, riferite a persone, **non possa trattare tali dati** se non con modalità che rispettino **tutte** le seguenti **istruzioni.**

Tali **istruzioni** sono da considerarsi, a tutti gli effetti, quali direttive provenienti dal proprio datore di lavoro e, in quanto tali, il loro mancato rispetto potrebbe generare delle responsabilità a carico del dipendente.

Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile mediante riferimento a qualsiasi altra informazione disponibile.

Dato particolare: i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

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.

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.

Autorizzati al trattamento: le persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, a prescindere dalla funzione svolta all'interno dell'Ateneo.

Postazione di lavoro: l'insieme degli strumenti informatici e non messi a disposizione dal datore di lavoro per rendere la prestazione lavorativa, sia in sede sia

[1] Art. 32, comma 4:
Il titolare del trattamento e il responsabile 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 dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

in mobilità (ad es. archivi, armadi, cassettiere, scrivanie, computer, stampanti, fax, telefoni cellulari di proprietà dell'Ateneo, ecc.).

Istruzioni

1. Accesso ai dati da parte di soggetti non autorizzati al trattamento

Occorre sempre **controllare** che l'**accesso** ai dati trattati dall'Ateneo in qualsiasi contesto (segreterie, uffici, divisioni/direzioni, dipartimenti, attività didattica e di ricerca, eventi) possa avvenire da parte di persone non autorizzate al trattamento, siano essi interni o esterni all'Ateneo. Il dato deve, innanzitutto, essere **protetto da accessi** non autorizzati, che possono avvenire di persona (si pensi a un soggetto non autorizzato che entra fisicamente in un ufficio e prova a conoscere o sottrarre dati) o tramite contatti telematici che possono rivelarsi truffaldini (ad esempio un'email o altra forma di presa di contatto mediante la quale si provino a raccogliere determinati dati o informazioni).
I documenti cartacei contenenti dati personali e tutta la documentazione amministrativa devono essere custoditi per evitare l'accesso agli stessi da parte di soggetti non autorizzati.

2. Sicurezza della postazione di lavoro

La postazione di lavoro deve essere configurata in modo che sia impostato l'avvio automatico dello screensaver ("salvaschermo") dopo al massimo 5 minuti di inattività del Personal Computer. È facoltà degli Autorizzati, qualora lo ritengano necessario od opportuno in ragione dei dati che stanno trattando, stabilire un intervallo temporale minore.

In caso di assenza momentanea dal proprio posto di lavoro, ci si deve accertare che la sessione di lavoro non sia accessibile a terzi, facendo **logout** o attivando il salvaschermo (screensaver) con blocco della sessione protetta da credenziali di autenticazione. Lasciare il proprio computer accessibile quando ci si allontana dalla propria scrivania genera una **vulnerabilità** molto pericolosa, e incontrollabile, al proprio lavoro e al patrimonio di dati dell'Ateneo.

Tutti i computer, sia desktop che portatili, **devono** avere installato e attivo il software **antivirus** dell'Ateneo (https://work.unimi.it/servizi/servizi_tec/6562.htm), con firewall attivato e devono essere mantenuti costantemente **aggiornati** con le patch di sicurezza del sistema operativo e degli applicativi utilizzati. Tali aggiornamenti sono, nella maggior parte dei casi, automatici e non richiedono l'intervento dell'utente. Non bisogna però, salvo casi eccezionali, bloccare o ritardare un aggiornamento dei software o dei sistemi, ma è necessario procedere immediatamente al salvataggio dei file eventualmente aperti e acconsentire all'aggiornamento. Le ulteriori misure di sicurezza richieste sono specificate nel Regolamento di Ateneo in materia di Sicurezza ICT e nelle linee guida e indicazioni reperibili nell'apposita sezione del Portale di Ateneo dedicata alla sicurezza informatica e protezione dati.

3. Spegnimento obbligatorio dei Personal Computer

Tutti i Personal Computer (desktop e portatili) di Ateneo che vengono usati nelle sedi universitarie, al termine delle ore di servizio, devono essere **spenti**, a meno che per particolari ragioni tecniche o di servizio debbano rimanere in funzione (in tal caso, il computer acceso deve risiedere in un ufficio o in un locale **chiuso** a chiave o protetto e con salvaschermo attivo e protetto da credenziali).

4. Protezione dei supporti esterni e dei dispositivi mobili

Particolare attenzione alla **custodia** deve riguardare anche i **supporti esterni** (es chiavette USB, dischi esterni, tablet, smartphone,) evitando di lasciarli in luoghi non protetti. Per i supporti esterni mobili è richiesto di utilizzare la **cifratura** dei dati. Maggiori informazioni sono disponibili sul portale di Ateneo nella sezione dedicata alla sicurezza informatica e alla protezione dei dati e in particolare all'indirizzo:
http://www.unimi.it/Guida%20alla%20cifratura%20dei%20dati_v1.pdf
https://work.unimi.it/filepub/sicurezza_ict/indicazioni_generali_cifratura_dati_v1.pdf

5. Controllo delle stampe e dei documenti

Occorre prestare attenzione alla **stampa** di documenti o alla ricezione di **fax** su stampanti condivise o fotocopiatrici di rete, avendo cura di recuperare tempestivamente la stampa e di non lasciare i documenti incustoditi. La protezione dei dati si applica anche a **documenti cartacei**, cui va garantita custodia e controllo. Non riutilizzare per appunti il retro di fogli stampati o fotocopiati se contengono dati personali. Qualora sia fornito, è sempre necessario utilizzare il "distruggi-documenti" per rendere non leggibili i documenti contenenti dati personali o informazioni rilevanti. Nel caso si debbano smaltire grandi moli di documenti cartacei connessi all'attività di ricerca e didattica (esempio documenti correlati a prove d'esame di studenti) e contenenti dati personali è necessario contattare l'Ufficio Servizio Prevenzione e Sicurezza sul Lavoro per fruire del servizio di gestione dei rifiuti.

6. Ulteriori cautele nella gestione del Personal Computer portatile

Non lasciare mai incustodito il computer portatile. Lo smarrimento, il furto, l'accesso non autorizzato o la sospetta manomissione di un computer **che contenga dati personali** comporta un cosiddetto *data breach*, ossia una violazione del patrimonio di dati dell'Ateneo, che deve essere **segnalato** immediatamente, e comunque al massimo entro **24 ore**, all'indirizzo **violazione.dati@unimi.it** affinché vengano svolti in tempo utile gli adempimenti di legge.
Se sono presenti dati personali di cui l'Ateneo è Titolare, sui **computer portatili** devono essere adottati meccanismi di **cifratura** dei dati al fine di ridurre il rischio

collegato al *data breach* in caso di smarrimento o furto del computer, seguendo le istruzioni già indicate al punto 4 del presente documento.

7. Gestione delle credenziali di accesso ai computer, ai dati e ai servizi

È obbligatorio impostare delle **credenziali di accesso** (username e password) **che** siano sicure, non note ad altri e mai comunicate a terzi, né a voce, né per e-mail, su siti non istituzionali o in chat. In particolare, la password deve essere **univoca** (non usata per più servizi, sistemi o siti), **robusta** (lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente), **cambiata frequentemente (almeno ogni 6 mesi) e regolarmente**, e sempre **diversa** da quelle utilizzate in precedenza. Non usare la stessa password usata per l'accesso ai sistemi e servizi universitari per accedere ad applicazioni o siti che siano esterni al dominio Unimi e connessi ad attività non istituzionali. Le password non devono essere mai scritte e conservate in luoghi e modi che non garantiscano adeguata protezione.

8. Atteggiamento diffidente nei confronti di qualsiasi richiesta di dati

Il dipendente deve mantenere sempre un atteggiamento **prudenziale** e rispondere sempre in maniera **negativa** a richieste di dati, effettuate in qualunque modo, che non pervengano chiaramente da soggetti autorizzati, e la cui identità, in caso di dubbio, non sia stata accuratamente verificata. Le richieste di dati devono avvenire obbligatoriamente in forma scritta e, nel caso, autorizzate dal proprio responsabile. È vietato, altresì, fornire o rendere disponibili **informazioni tecniche**, riferite alla rete e ai sistemi di Ateneo, alle policies e alle credenziali usate, ai software e alle applicazioni utilizzate, a soggetti esterni all'Ateneo. Tali informazioni sono solitamente domandate per cercare di violare i sistemi di Ateneo con la tecnica del *social engineering*.

9.Salvataggio (backup) dei dati

È obbligatorio adottare tutte le misure necessarie per salvaguardare i dati mediante regolari backup e per consentirne il ripristino nel caso di perdita accidentale o sottrazione del dispositivo, cancellazione accidentale o alterazione dei dati. La copia di backup deve essere custodita offline (scollegata dal sistema che ospita i dati), in un luogo sicuro e cifrato in considerazione della natura e quantità dei dati. È vietato utilizzare servizi di archiviazione e condivisione file per backup offerti da operatori commerciali (ad es. Google Drive, Dropbox, iCloud, OneDrive), se non espressamente previsti da una lista autorizzata dall'Ateneo. E' altresì incoraggiato l'uso degli strumenti messi a disposizione dalle strutture tecniche di Ateneo.

10. Minimizzazione nell'utilizzo dei dati personali

I dati personali degli interessati devono essere utilizzati il **meno possibile**, non diffusi a soggetti terzi, cancellati non appena la politica d'Ateneo lo consente, e

particolare attenzione va portata nei confronti di dati classificati come *particolari* (già dati *sensibili*). Nel momento in cui il dipendente venga a conoscenza di un trattamento non corretto, eccedente le finalità, inutile o pericoloso, deve per il tramite del responsabile di Struttura, segnalarlo al Data Protection Officer e all'Ufficio Sicurezza ICT all'indirizzo **violazione.dati@unimi.it**.

Riferimenti e approfondimenti

Per gli approfondimenti e aggiornamenti di quanto descritto nel presente documento, e per le modalità di implementazione delle misure di sicurezza richieste, fare riferimento ai documenti dell'Ufficio di Sicurezza ICT di Ateneo pubblicati sul portale nella sezione dedicata alla sicurezza e protezione dei dati personali a partire dalla URL: https://work.unimi.it/servizi/security_gdpr/118546.htm
Il materiale divulgativo in tema di protezione dei dati personali è disponibile sul sito di Ateneo nell'apposita sezione dedicata alla sicurezza informatica e protezione dei dati personali a partire dalla URL:
https://work.unimi.it/servizi/security_gdpr/118604.htm