UNIVERSITÀ DEGLI STUDI DI MILANO

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

L'Università degli Studi di Milano, in qualità di titolare del trattamento dei dati personali dell'Ateneo, dispone che chiunque abbia accesso a dati personali, 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, al fine di proteggersi da eventuali violazioni dei dati (**DATA BREACH**) **non possa trattare tali dati** se non con modalità che seguano **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.

ISTRUZIONI

1. Individuare un data breach (violazione dei dati)

Per data breach (o violazione dei dati personali) si intende un incidente di sicurezza[2] 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.
Ciascun dipendente, coinvolto in una presunta violazione dati che abbia colpito il suo sistema o il suo ufficio, deve segnalare la violazione dei dati personali nel più breve tempo possibile, entro 4-6 ore e comunque non oltre le 24 ore.
Un tipico data breach consiste in: a) furto o smarrimento di un computer fisso o di un dispositivo portatile (es. pc portatile, disco removibile, pen-drive USB); b) accesso dall'esterno ai dati di Ateneo da parte di un criminale informatico; c) distruzione o alterazione accidentale di dati e informazioni; d) divulgazione di dati confidenziali a persone non autorizzate; e) perdita o furto di documenti cartacei; f) divulgazione al pubblico di dati riservati; g) virus o altri attacchi al sistema informatico o alla rete di ateneo; h) violazione di misure di sicurezza fisica quali, ad esempio, la forzatura di porte o finestre di particolari locali (sale macchine, depositi dei nastri del backup, locale che ospita il server NAS, archivi anche cartacei, locali contenenti informazioni riservate); i) invio accidentale di e-mail contenenti dati personali e/o particolari al destinatario sbagliato; m) in generale, qualsiasi situazione che possa portare un soggetto non autorizzato alla conoscenza o disponibilità di dati personali.

2. Comportamento in caso di furto o smarrimento di computer o dispositivi

Nel caso in cui un computer fisso, un pc portatile, un hard disk, una chiavetta USB o altri supporti di memoria fossero oggetto di **furto** o **smarrimento**, occorre segnalare immediatamente l'avvenimento al Data Protection Officer e all'Ufficio Sicurezza ICT inviando un'email a: **violazione.dati@unimi.it**.

[1] (*)Art. 32, comma 4 del Regolamento Generale per la Protezione dei Dati (EU 2016/679): 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.

[2] Un incidente di sicurezza è un evento identificato o un punto di debolezza che indica una possibile violazione delle politiche di sicurezza, un fallimento delle misure di protezione o una situazione precedentemente sconosciuta con impatto sulla sicurezza informatica. Un esempio di incidente di sicurezza si può verificare quando un utente è indotto ad aprire un file allegato alla mail che in realtà è un virus; l'esecuzione del virus comporta l'infezione del dispositivo stabilendo connessioni con un host esterno;

3. Comportamento in caso di altri incidenti informatici

Vanno segnalati anche tutti gli incidenti comunque **correlati** ai dati, quali furto di informazioni effettuate online, cancellazione accidentale di informazioni, comunicazione di informazioni a terzi per errore. Ciò anche se non vi sia stato un comportamento criminale alla base ma un evento accidentale.

4. Data breach correlato al phishing

Va inteso come data breach anche un attacco di **phishing** che sia andato a buon fine, ossia l'aver fornito e diffuso credenziali e dati tecnici a un soggetto terzo (v. in tal senso le istruzioni d'Ateneo per il contrasto al phishing).

5. Denunciare qualsiasi tipo di incidente all'Ateneo

È opportuno segnalare qualsiasi tipo di incidente di sicurezza, anche **lieve o connesso ai dati personali**, sia al referente tecnico di struttura, qualora presente, sia all'Ufficio Sicurezza ICT per consentine la gestione e valutarne la gravità e le conseguenze normative.
Ciò consentirà all'Ateneo di mantenere un **registro degli incidenti** aggiornato, che consenta una costante analisi del rischio e di predisporre misure di prevenzione.

6. L'esigenza di tempestività nella denuncia

Il Regolamento Generale sulla Protezione dei Dati richiede, in caso di data breach, l'attivazione, da parte dell'Ateneo, di una procedura che deve essere **rapida** e contenuta nelle **72 ore** massimo. È, perciò, d'obbligo per il dipendente segnalare ai vertici dell'Ateneo qualsiasi situazione connessa alla violazione dei dati (anche sospetta) entro 4-6 ore dall'accadimento e comunque non oltre 24 ore.

7. Fornire informazioni dettagliate per una prima quantificazione del danno

È importante, in caso di incidente, fornire agli uffici preposti alla gestione delle violazioni dei dati personali informazioni **veritiere** e le più **dettagliate** possibile su ciò che è accaduto, compilando l'apposito modulo pubblicato nella sezione del portale di Ateneo dedicata alla "Sicurezza informatica e protezione dei dati personali" a partire dalla URL:
https://work.unimi.it/servizi/security_gdpr/118546.htm
Le informazioni più importanti sono:

- che tipo di dati sono coinvolti;
- se sono stati coinvolti anche dati *particolari* (ex *sensibili*);
- quanti soggetti sono coinvolti;
- che estensione ha avuto l'incidente;
- il periodo temporale coinvolto;
- le misure di sicurezza adottate;
- se i dati fossero cifrati o meno.

8. Cifratura dei dati

La **cifratura** dei dati, memorizzati in file system e degli smartphone, nonché dei supporti esterni, aiuta a difendersi da eventuali data breach, così come l'uso di **credenziali forti** (lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente). È quindi obbligo per ciascun dipendente valutare l'adozione della **cifratura**[3] o di pseudonimizzazione[4] dei dati che gestisce e di adottare credenziali robuste per l'accesso a tali sistemi. Nell'implementazione delle misure ciascun utente può chiedere supporto al referente tecnico di struttura, ove presente. L'Ateneo ha elaborato indicazioni tecniche per favorire gli utenti nell'implementazione della cifratura reperibili nella sezione del portale dedicata alla "Sicurezza informatica e protezione dei dati personali" in "Regolamenti e linee guida".

9. Prestare attenzione al flusso di informazioni necessario per denunciare

La denuncia all'Ateneo di una violazione dei dati deve generare un **flusso** di informazioni efficiente ed organico per permettere all'Ateneo di reagire con prontezza e di evitare sanzioni.

10. Modalità di comunicazione della violazione

Per comunicare una violazione, in ottemperanza alla circolare Rettorale n. 60/2018, bisogna inviare senza ingiustificato ritardo una e-mail all'indirizzo **violazione.dati@unimi.it** mettendo in **copia per conoscenza** il proprio responsabile di struttura e garantendo la massima sollecitudine.
Inviata la mail di segnalazione, occorre poi compilare tempestivamente l'apposito modulo, coadiuvato, ove presente, dal referente della struttura di appartenenza. Il modulo di segnalazione è disponibile sul portale di Ateneo https://work.unimi.it/ alla voce "Violazione di dati personali (data breach)" presente nella sezione dedicata alla "Sicurezza Informatica e protezione dati personali".

Riferimenti e approfondimenti

Per gli approfondimenti e aggiornamenti di quanto descritto nel presente documento, per le modalità di implementazione delle misure di sicurezza richieste e per la consultazione del materiale divulgativo in tema di protezione dei dati personali e sicurezza informatica, fare riferimento ai documenti dell'Ufficio di Staff Sicurezza ICT ("Cybersecurity, Protezione Dati e Conformità" dal 01-01-2020) di Ateneo pubblicati sul portale di Ateneo nella sezione dedicata alla "Sicurezza informatica e protezione dei dati personali" a partire dalla URL: https://work.unimi.it/servizi/security_gdpr/118546.htm.

[3] La cifratura è una tecnica che permette di rendere intellegibile il contenuto dei dati in modo che essi possano essere correttamente compresi solo da chi ne possiede la chiave di decifratura posseduta solo dalle persone autorizzate.

[4] La pseudoanonimizzazione è una tecnica che consiste nel conservare i dati in una forma tale da impedire l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive. Ad esempio sostituire il nome di un paziente con un codice (alfanumerico) e tenere separata la tabella di risoluzione che permette di risalire all'identità dell'interessato.