UNIVERSITÀ DEGLI STUDI DI CATANIA

SICUREZZA E PROTEZIONE DEI DATI PERSONALI

Il presente documento individua le politiche di sicurezza a salvaguardia dei dati personali, di cui l'Università degli Studi di Catania è titolare, detenuti nelle banche dati, nonchè dei trattamenti effettuati in maniera informatizzata presso tutte le strutture dell'Ateneo, secondo quanto dettato da Decr. Lgs 196/2003 "Codice in materia di protezione dei dati personali".

Per maggiore chiarezza sono qui di seguito richiamate determinate definizioni di cui all'art.4 del Decreto citato:

omissis...

1 . Ai fini del presente codice si intende per:

*a) "**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;*

*b) "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*

*c) "**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;*

*d) "**dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*

*e) "**dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;*

*f) "**titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;*

*g) "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;*

*h) "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*

*i) "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;*

*l) "**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;*

*m) "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.*

Omissis...

SICUREZZA:

Il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;
Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;
Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

UNIVERSITÀ DEGLI STUDI DI CATANIA

DECALOGO

IN MATERIA DI SICUREZZA E DI PROTEZIONE DEI DATI PERSONALI

1) Il primo livello di protezione è fisico: mantenete sotto chiave i documenti cartacei dopo averli utilizzati.
2) Gli archivi devono essere custoditi in luoghi ad "accesso selezionato", cioè in locali in cui non hanno accesso diretto soggetti estranei.
3) Riducete al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
4) Mantenete tutti i documenti cartacei fuori dalla portata dei soggetti che non sono interessati al singolo procedimento amministrativo; al termine del loro utilizzo abbiate cura di distruggerli prima di cestinarli.
5) Poiché una parte consistente dei dati è trattata attraverso procedure informatiche, utilizzate credenziali di autenticazione personale (user id e password) di accesso al vostro pc, nonché abilitate la funzione che impone la digitazione della password al ripristino dopo alcuni minuti di inattività.
6) Effettuate ad intervalli regolari e frequenti le copie di sicurezza dei dati (backup), per salvaguardarli da eventi accidentali (perdita, danneggiamento, virus) e custodirle in luogo sicuro.
7) Evitate di installare software sul personal computer di lavoro prima di aver consultato l'amministratore di sistema.
8) Mantenete periodicamente aggiornati il sistema operativo e l'antivirus.
9) Per limitare lo spamming, evitate di comunicare o diffondere il vostro indirizzo di posta elettronica in Internet; cestinate le email, ivi compresi gli allegati, che provengono da sconosciuti.
10) Ricordate che i dati personali oggetto di trattamento devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e/o successivamente trattati.

Per quanto qui non espressamente citato si richiama la normativa vigente, il Documento Programmatico sulla Sicurezza dei dati 2007 e il Vademecum per la sicurezza dei dati personali dell'Università di Catania.

Si rammenta che la mancata applicazione della normativa vigente in materia di Privacy, espone al rischio di pesanti sanzioni amministrative (artt. 161, 162, 163 e 164 del D.Lgs 196/03) e penali (artt. 167, 168, 169, 170 e 171 del D.Lgs 196/03).
In particolare, per il trattamento illecito di dati è prevista la reclusione da 6 mesi a 3 anni; per mancata adozione delle misure di sicurezza è previsto l'arresto sino a 2 anni o un'ammenda da €. 10.000,00 a €. 50.000,00.

Il Responsabile della Sicurezza Informatica
Presidente del CEA
Prof. Avv. Bruno Caruso