UNIVERSITÀ DEGLI STUDI DI SIENA

ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI, SENSIBILI E/O GIUDIZIARI

In ottemperanza alle disposizioni del Codice in materia di protezione dei dati personali (D.Lgs 196/03), al Regolamento di Ateneo di attuazione delle norme in materia di trattamento dei dati sensibili e giudiziari, al Documento Programmatico per la Sicurezza di Ateneo (consultabili sul sito web dell'Ateneo, alla pagina www.unisi.it/ateneo/privacy), ed in relazione alle attività svolte nell'ambito della Struttura universitaria di appartenenza, l'Incaricato dovrà effettuare i trattamenti di dati personali di propria competenza, attenendosi scrupolosamente alle seguenti istruzioni ed ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Responsabile del trattamento.

I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza, nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato;

b) in modo lecito e secondo correttezza;

c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le *misure minime di sicurezza* (di cui agli artt. 33 – 36 ed allegato B del citato D.lgs.196/03) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. Senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);

2. Con strumenti elettronici (PC ed elaboratori).

1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Le misure di sicurezza applicate alle copie o alle riproduzioni, il cui numero deve in ogni caso essere limitato all'effettiva necessità, dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

1.1 Custodia

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

1.2 Comunicazione

- L'utilizzo dei dati personali deve avvenire in base al "principio di necessità" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi se non previa autorizzazione del Responsabile.

1.3 Distruzione

- Qualora sia necessario distruggere le copie o le riproduzioni di documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

• I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

1.4 Ulteriori istruzioni in caso di trattamento di dati sensibili e/o giudiziari

• I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Incaricati in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.

• L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

• Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

2. TRATTAMENTI CON STRUMENTI ELETTRONICI

2.1 Gestione delle credenziali di autenticazione

• La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (*user-id*) associato ad una parola chiave riservata (*password*), oppure in un dispositivo di autenticazione (es. *smart card*). Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

• Le *user-id* individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile del trattamento.

• Gli strumenti di autenticazione (ad esempio, le password) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Incaricati del trattamento).

• Le *password* devono essere sostituite, a cura del singolo Incaricato, al primo utilizzo e successivamente almeno ogni sei mesi.

• Le *password* devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le *password* non devono contenere riferimenti agevolmente riconducibili all'Incaricato (es. nomi propri e di familiari).

2.2 Protezione del PC e dei dati

• Tutti i PC devono essere dotati di password.

• Tutti i PC devono essere dotati di software antivirus aggiornato costantemente.

• Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle strutture di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente.

• Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password.

• Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.

• Deve essere effettuato, con cadenza almeno settimanale un salvataggio di *back-up* di eventuali dati personali presenti unicamente sul PC personale (cioè non accessibili tramite i sistemi informatici universitari). I supporti di memoria utilizzati per il *back-up* devono essere trattati secondo le regole definite al punto "Trattamento senza l'ausilio di strumenti elettronici".

2.3 Cancellazione dei dati dai PC

• I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

2.4 Custodia

• I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

2.5 Ulteriori istruzioni in caso di trattamento di dati sensibili e/o giudiziari

• Le *password* di accesso alle procedure informatiche che trattano dati sensibili e/o giudiziari devono essere sostituite, da parte del singolo incaricato, almeno ogni tre mesi.

• L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuato almeno semestralmente.

3. ISTRUZIONI DI CARATTERE GENERALE

3.1 Come scegliere e usare la password (Normativa sulla costruzione ed utilizzo delle password)

• Usare almeno 8 caratteri, o nel caso in cui lo strumento elettronico non lo permetta, usare un numero di caratteri pari al massimo consentito.

• Non utilizzare date di nascita, nomi o cognomi propri o di parenti.

• Non sceglierla uguale alla matricola o alla *user- id.*

• Custodirla sempre in un luogo sicuro e non accessibile a terzi

• Non divulgarla a terzi

• Non condividerla con altri utenti

3.2 Come comportarsi in presenza di ospiti o di personale di servizio

• Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.

• Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salva schermo del PC.

• Non rivelare o fare digitare le *password* dal personale di assistenza tecnica.

• Non rivelare le *password* al telefono né inviarla via fax - nessuno è autorizzato a chiederle.

• Segnalare qualsiasi anomalia o stranezza al Responsabile.

3.3 Come gestire la posta elettronica

• Non aprire messaggi con allegati di cui non si conoscono l'origine, possono contenere virus in grado di cancellare i dati sul PC.

3.4 Come usare correttamente Internet

• Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro, in quanto questo può essere pericoloso per i dati e la rete d'Ateneo. I software necessari all'attività lavorativa vanno richiesti alle competenti strutture universitarie.

4. SANZIONI PER INOSSERVANZA DELLE NORME

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy; l'inosservanza delle quali da parte dell'Incaricato può comportare sanzioni anche di natura penale a suo carico ai sensi delle disposizioni di cui alla parte III, titolo III, capi I e II del D.Lgs. N. 196/2003 (artt. da 161 a 172 del D. Lgs. 196/2003).