Fondazione Eni Enrico Mattei

NORME DI COMPORTAMENTO DEGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

ISTRUZIONI AGLI INCARICATI

ISTRUZIONI PER GLI INCARICATI

Nel seguito sono descritte le prescrizioni alle quali Lei dovrà attenersi nello svolgimento dei compiti che le sono stati affidati.

I dati personali oggetto di trattamento devono essere:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) 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 essi sono stati raccolti o successivamente trattati.

Sarà Sua cura effettuare le operazioni di trattamento che Le vengono affidate, nel rispetto delle disposizioni di legge, verificando in particolare che ai soggetti interessati sia stata data l'informativa e ne sia stato ottenuto, ove previsto, il consenso.
Dovrà inoltre verificare che il consenso non sia stato revocato.

Nel caso in cui i dati trattati siano raccolti presso terzi, sarà Sua cura verificare che i dati siano stati raccolti correttamente e che sia stata rilasciata opportuna informativa e ove previsto, il consenso dell'interessato.

Cosa fare	Cosa non fare
Trattamento illecito	
• Effettuare solo trattamenti di dati per i quali si è stati autorizzati • Segnalare immediatamente trattamenti che non si ritiene conformi a quanto dichiarato nell'informativa rilasciata all'interessato o quando si ritiene che non sia stato espresso il consenso da parte dell'interessato	• Effettuare trattamenti non consentiti o non conformi, sia per propria iniziativa sia su indicazione di terzi
Cessazione del rapporto di lavoro	
• In caso di cessazione del rapporto di lavoro è necessario riconsegnare dati e strumenti all'azienda	• Comunicare a terzi, anche successivamente alla cessazione del rapporto di lavoro dati, informazioni, documenti
Esattezza dei dati	
• Nella trascrizione, caricamento, elaborazione, stampa, inoltro… dei dati devono essere effettuati gli opportuni controlli al fine di verificarne la correttezza	

ACCESSO AI DATI

L'acceso ai dati può avvenire unicamente da parte di personale che abbia ricevuto:

- specifica lettera di incarico
- idonea formazione

In particolare Lei potrà accedere unicamente ai dati (con o senza l'utilizzo di strumenti elettronici) strettamente necessari per lo svolgimento dei trattamenti per i quali Lei è stato autorizzato.

L'accesso ai sistemi informativi avviene mediante specifiche credenziali di autenticazione e profili di autorizzazione.

L'accesso agli archivi non informatizzati è selezionato.

L'accesso agli archivi non informatizzati di dati sensibili e giudiziari è selezionato e controllato, e può avvenire solo durante l'orario di lavoro, salvo preventiva autorizzazione e registrazione sull'apposito registro.

ACCESSO AI LOCALI

L'accesso ai locali di FEEM per gli incaricati può avvenire di norma dalle ore 8 alle ore 19,30.
L'accesso da parte di terzi per operazioni di manutenzione impianti ed attività ad esse comparabili (elettricisti, idraulici…) può avvenire unicamente previa consegna di lettera di riservatezza. Tale adempimento può essere effettuato anche una sola volta in fase di conclusione del contratto con la controparte.

L'accesso di partner, fornitori e più in generale dei visitatori deve limitarsi ai locali aperti al pubblico.
Tali soggetti possono accedere solo accompagnati ai locali nei quali si svolgono trattamenti di dati comuni, solo dopo aver provveduto a rendere inaccessibili i dati di terzi.
Tali soggetti non possono in alcun modo accedere ai locali nei quali si svolgono trattamenti di dati sensibili o giudiziari.

STRUMENTI AZIENDALI E STRUMENTI PERSONALI

Gli strumenti aziendali possono essere utilizzati solo per finalità lavorative.
È consentito l'uso del telefono aziendale per fini personali unicamente per casi di necessità.
È vietato di norma, l'uso di qualunque strumento personale, ivi compresi palmari.

SEGNALAZIONI IN CASO DI ANOMALIA

In caso di malfunzionamenti del sistema informativo, dovrà darne immediata segnalazione all'Ufficio ICT o al Titolare.

SEGNALAZIONI IN CASO DI FURTO

In caso di furto di strumenti aziendali dovrà darne immediata segnalazione ai Servizi Generale.

ECCEZIONI ALLE REGOLE GENERALI

Eventuali eccezioni sull'uso di strumenti aziendali o personali rispetto al contenuto del seguente regolamento devono essere preventivamente concordati e segnalati ai Servizi Generali e Servizi ICT per la relativa valutazione di impatto.

Pc di lavoro e sistema informativo

Cosa fare	Cosa non fare
Pc di lavoro	
• Utilizzare la propria postazione diligentemente ed unicamente per le finalità aziendali • Segnalare subito eventuali malfunzionamenti • Spegnere il pc al termine del lavoro	• Modificare la configurazione del pc • Installare software se non fornito dall'azienda • Caricare dati, se non forniti dall'azienda • Installare periferiche, se non fornite dall'azienda
Pc a casa	
• Attrezzare in luogo adatto la posizione di telelavoro, al fine di garantire la sicurezza	• Consentire ad altri l'uso della postazione
Accesso al sistema informativo	
• Utilizzare user id e password personale	
Password personale	
• Impostare la password (o le password) personale secondo le regole più avanti riportate • Modificare la password assegnata al primo utilizzo • Modificare la password almeno ogni 6 mesi (3 mesi per trattamento di dati sensibili) • Segnalare immediatamente al Titolare il sospetto che terzi siano entrati in possesso della password	• Comunicare a chiunque la propria password salvo che non sia espressamente richiesta la sua comunicazione in forma segreta al custode delle password (che ne ha copia, ma non la conosce)

Alcune regole base per la costruzione della password riguardano:

- lunghezza minima (8 caratteri utenti - 16 nel caso di utenti con privilegi amministrativi)
- contenere sia caratteri maiuscoli che minuscoli
- contenere sia lettere che numeri
- contenere simboli speciali (non alfanumerici)
- non avere alcun riferimento con l'incaricato che la utilizza
- non contenere parte della user id
- non deve essere una parola di senso compiuto
- non deve essere una sequenza di tasti adiacenti
- non deve essere comunicata a nessuno
- non deve essere scritta da nessuna parte
- non digitare la password quando sono presenti terzi

Una regola molto semplice che porta alla creazione di password forti facilmente memorizzabili è quella di fare riferimento a frasi di senso compiuto delle quali si utilizzino le iniziali.

Ad esempio "la distanza fra casa mia e il posto di lavoro è di 60 chilometri" può portare alla creazione di una password di questo tipo: **"ldfcmeipdlèd60c",** che si può ulteriormente complicare con l'uso di simboli speciali ad esempio all'inizio ed alla fine: **"#ldfcmeipdlèd60c%"**
È inoltre consigliabile l'uso di maiuscole e minuscole: **#Ldfcmeipdlèd60C%"**
La password risultante è molto complessa, ma anche molto facile da ricordare.

I 10 FATTORI DI SICUREZZA DELLA PASSWORD

La password assegnata dovrà rispettare i 10 fattori di sicurezza riguardante i criteri minimi accettabili per la gestione delle password (normativa americana), in particolare:

1) Composizione
Avere una base assai larga di parole accettabili, contro tentativi di ricerca e sperimentazione di parole accettabili
La legge prevede un minimo di almeno 8 caratteri. E' consentito l'utilizzo di una parola chiave solo con caratteri numerici, anche se questa scelta porta a un livello inferiore di sicurezza, rispetto a una scelta alfanumerica.

2) Lunghezza
La lunghezza stabilisce i limiti della sicurezza potenziale del sistema. Una lunghezza pari a 2 porta questo numero al quadrato; pari a 3 porta il numero all'esponente cubico;

3) Vita utile
Le parole chiave devono essere cambiate su base periodica e ogni qualvolta vi sia un sospetto di compromissione. La legge indica la vita utile minima in 6 mesi, con riduzione a 3 mesi in caso di dati giudiziari o sensibili.
I sistemi di parole chiave devono avere la possibilità di sostituire la parola rapidamente, con procedura avviata dall'utente o dal gestore del sistema di sicurezza.

4) La scelta
Il disciplinare prevede la adozione di una tecnica di sicurezza "one off" oppure "one time password": questa tecnica consente nel generare, presso un servizio centrale, generalmente controllato dal Titolare del trattamento, la parola chiave. Essa viene utilizzata per il primo accesso al sistema di trattamento. Tale parola può essere utilizzata una sola volta e il sistema, appena digitata la parola, invita l'incaricato a sostituirla immediatamente.

5) La titolarità
La parola chiave deve essere di proprietà individuale. Questa imposizione è fondamentale perché:
stabilisce una responsabilità individuale
conferma l'uso illecito di una parola chiave
può essere utilizzata per ricostruire l'attività svolta da un incaricato
evita di cambiare la parola chiave a un intero gruppo quando un singolo si allontana dal gruppo stesso

6-7) La distribuzione e la modifica
La parola chiave è inizialmente creata e distribuita per iscritto. Se vi è una spedizione non deve contenere segni riconoscibili o di identificazione del contenuto e deve essere riservata all'incaricato. Deve essere fatta la raccomandazione che la parola chiave sia utilizzata al più presto e immediatamente modificata.

8) L'archiviazione
Le parole chiave devono essere archiviate nel sistema di autenticazione in modo da minimizzare la esposizione alla rivelazione o alla sostituzione non autorizzata. Sono stati individuati molti sistemi per proteggere le parole chiave in memoria. Alcuni sistemi hanno un file di parole chiavi, che può essere letto solo dal programma LOGON. Il file è protetto da un meccanismo di controllo che verifica la presenza di un bit di protezione nella tavola di accesso. Solo il programma privilegiato può leggere il file e solo il programma di gestione delle parole chiave può scrivere il file.
Altri sistemi cifrano le parole chiave, sia in modo reversibile che irreversibile, usando un algoritmo DES con chiave DEK, con la parola chiave stessa come chiave. Ogni parola chiave mantenuta in archivio deve essere protetta da un ulteriore chiave di cifratura, la cosiddetta KEK.
La parola chiave introdotta da un utente può essere confrontata con la parola decifrata, oppure la parola chiave dell'utente può essere confrontata con la parola già archiviata.

9) La digitazione
Il terminale del computer e la tastiera devono essere dotati di mezzi che possono minimizzare l'esposizione della parola chiave, durante la digitazione. Le parole chiave non devono apparire sul video terminale durante la digitazione. La parola chiave deve essere mascherata e non visualizzata, mostrando – ad esempio – degli asterischi nello spazio dove la parola chiave può essere stampata. La parola chiave non deve in nessun caso rimanere nella memoria del computer, e neanche essere stampata su supporti di qualsiasi tipo, dopo la digitazione e verifica.
Il sistema deve anche impedire dei tentativi rapidi e ripetuti, quando una parola chiave è digitata in modo non corretto. Devono passare alcuni secondi, prima di nuovo tentativo. Questo accorgimento impedisce un attacco automatizzato ad alta velocità, di tipo esaustivo. E' bene conservare una registrazione del fatto che sono state introdotte delle parole chiave errate.

10) La trasmissione
La parola chiave normalmente viene trasmessa dal terminale al computer tramite linee di comunicazione , che collegano il terminale al computer. La parola chiave è soggetta a intercettazione. A questo proposito, vi sono disponibili 2 metodi di cifratura.
Nel primo caso, la linea di comunicazione tra il terminale e il computer può essere protetta da apparati cifranti, che utilizzano una chiave segreta per cifrare le comunicazioni tra il terminale e il computer. Le parole chiave in trasmissione sono protette da rivelazione.
Nel secondo caso la parola chiave può essere utilizzata come chiave di cifratura o come parte di una chiave di cifratura.

CASI PARTICOLARI

Pc con utente amministrative

• Gli utenti che per esigenze lavorative sono dotati di PC con utenze amministrative devono rispettare comunque le presenti regole, in particolare per quanto attiene l'uso del pc ai soli fini aziendali e l'installazione di software preventivamente autorizzato.	• Installare software non autorizzato • Utilizzare il pc per fini personali • Caricare file personali

VERIFICA DEL RISPETTO DELLE PRESCRIZIONI AZIENDALI

Durante l'attività di manutenzione dei pc con utenze amministrative il personale dell'Ufficio ICT provvederà a verificare il rispetto delle prescrizioni aziendali, in particolare per quanto attiene l'installazione di applicazioni non preventivamente autorizzate, che verranno rimosse.

Uso di Pc con sistema operativo non standard

- Gli utenti che per esigenze lavorative utilizzano PC con sistemi operativi non standard (ad esempio Apple) sono comunque tenuti al rispetto delle presenti disposizioni.
- La dove tali disposizioni non sono implementate a livello tecnico (ad esempio lunghezza e scadenza password) sono tenuti ad impostarle manualmente.

Uso di Pc non aziendali

- Gli utenti che per esigenze lavorative utilizzano PC non aziendali sono comunque tenuti al rispetto delle presenti disposizioni allorquando trattano dati personali di cui è Titolare o Responsabile FEEM.
- L'uso di strumenti personali per effettuare trattamenti di dati personali di FEEM va concordato con i Servizi Generali e ICT.

Cosa fare	Cosa non fare
Antivirus [*]	
• Verificare costantemente l'aggiornamento dell'antivirus ed attivare la scansione dopo ogni aggiornamento • Scansionare qualunque supporto proveniente dall'esterno dell'azienda o destinato all'esterno dell'azienda sulle postazioni dotate di antivirus aggiornato • Segnalare subito i malfunzionamenti	• Utilizzare supporti provenienti dall'esterno senza averli adeguatamente verificati
Copia dei dati locali da parte degli utenti	
I dati presenti sulle postazioni utente non sono soggetti a copia di backup automatizzata. E' pertanto responsabilità del singolo utente provvedere alla loro copia. L' Ufficio ICT fornirà al riguardo la necessaria consulenza, se richiesta.	
• Copiare i dati con frequenza adeguata • Usare supporti per la copia a rotazione • Verificare periodicamente il ripristino dai supporti • Conservare i supporti in luogo sicuro diverso da quello dove sono conservati i dati principali	• Effettuare copie se non autorizzati • Usare sempre lo stesso supporto • Conservare la copia dei dati nello stesso luogo in cui sono conservati i dati originali
Supporti rimuovibili	
• Etichettare i supporti • Riutilizzare i supporti rimuovibili (floppy., ZIP, CD…) solo per lo stesso tipo di trattamento • Distruggere i supporti secondo quanto previsto dalla normativa **(Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali -13/10/ 2008)**	• Utilizzare, per uso personale, qualunque supporto rimuovibile, compresi token USB
Aggiornamento sistemi	*[L'aggiornamento è in carico all'Ufficio ICT]*
	• Effettuare aggiornamenti di propria iniziativa
Blocco della postazione	
• Ogni volta che ci si allontana dalla postazione questa deve essere bloccata (screen saver con password o altro)	
File personali	
	• Caricarli ed utilizzarli
Utilizzo di portatili o palmari	
• Oltre alle regole generali descritte in precedenza tutti i dati presenti sui dispositivi portatili devono essere crittografati	• Lasciare incustodito il dispositivo portatile in qualunque luogo (auto…)
Uso delle apparecchiature	
• Spegnere gli strumenti elettronici al termine dell'uso se non diversamente specificato	

Cosa fare	Cosa non fare
Internet	
• Accedere solo a siti per finalità lavorativa • Utilizzare solo la connessione fornita dall'azienda	• Accedere a siti sconosciuti • Scaricare file per finalità non attinenti all'attività lavorativa • Iscriversi a forum, chat, mailing list… utilizzando i riferimenti aziendali • Ascoltare programmi radio e musicali, conversazioni in chat line, collegamenti a webcam • Effettuare alcun genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on line e simili se non preventivamente autorizzati dalla Direzione • Connettersi alla rete di FEEM mediante dispositivi personali
Uso di servizi internet: dropbox	
	• Caricare dati personali unicamente a dati aziendali • Unire la casella personale a quella aziendale • Caricare materiale considerato riservato

Comunicazioni

Cosa fare	Cosa non fare
Telefono	
• Fornire solo le informazioni per le quali si è stati esplicitamente autorizzati • Segnalare al proprio responsabile richieste inusuali di informazioni • Nel caso di comunicazioni in viva voce informare l'interlocutore dell'attivazione di tale modalità e della presenza di eventuali altri ascoltatori; verificare in questo caso la presenza di terzi non autorizzati	• Fornire informazioni sulle misure di sicurezza in atto • Fornire informazioni sull'organizzazione aziendale • Fornire le proprie credenziali di autenticazioni • Fornire informazioni relative agli interessati a terzi non autorizzati
Segreterie telefoniche	
	• Lasciare informazioni riservate sulle segreterie telefoniche
Cellulari	
• Utilizzare password di accesso per la protezione della rubrica e dei dati • Bloccare il cellulare in caso di perdita o furto	• Effettuare registrazioni audio, video o fotografiche mediante cellulari, palmari o altri dispositivi se non autorizzati
Fax in uscita [*]	
• Controllare il numero di telefono chiamato • Aggiungere avvertenza su riservatezza sui documenti inoltrati • Verificare il corretto inoltro • Cancellare la memoria	• Dimenticare i documenti inoltrati e relativa ricevuta • EFFETTUARE INOLTRI AUTOMATIZZATI SENZA CONSENSO DEGLI INTERESSATI
Fax/posta in entrata	
• Controllare il destinatario (azienda) prima di accedere ai documenti • Controllare il destinatario (interno) prima di accedere ai documenti • Cancellare la memoria	• Accedere a documenti dei quali non si è destinatari
Posta convenzionale in uscita	
• Controllare che il destinatario sia corretto • Utilizzare una modalità di trasmissione congruente alla tipologia di dato (esempio: assicurata per dati sensibili)	

[*] Le stampanti multifunzione possono disporre della funzione di inoltro, anche via e-mail, dei documenti digitalizzati

Cosa fare	Cosa non fare
Posta elettronica [*]	
• La posta elettronica è utilizzabile solo per fini aziendali • Nel caso di inoltro a più destinatari utilizzare come indirizzo di destinazione quello dell'azienda e mettere in CCN i singoli destinatari, per evitare che un destinatario possa conoscere l'indirizzo degli altri • Utilizzare il disclaimer riportato più avanti • L'invio di comunicazioni ufficiali o contenenti impegni contrattuali e precontrattuali deve essere autorizzata dalla Direzione	• Utilizzare l'indirizzo aziendale a fini personali • INOLTRARE IN AUTOMATICO E-MAIL SENZA CONSENSO DELL'INTERESSATO • Aprire e-mail e file provenienti da mittenti sconosciuti • Utilizzare l'e-mail per l'inoltro o ricezione di dati sensibili, giudiziari o riservati • Inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica
Posta elettronica certificata [**]	
• L'uso della PEC è limitato agli utenti autorizzati • Verificare periodicamente la casella di PEC	

[*] La posta elettronica non fornisce garanzia di consegna al destinarlo e non da alcuna garanzia di riservatezza del messaggio.
L'uso dell'e-mail e la sua valenza ai fini contrattuali con le controparti deve essere regolamentata

[**] La PEC ha lo stesso valore della raccomandata r.r. fra due caselle di PEC; il suo utilizzo deve sottostare alla medesime regole aziendali che riguardano l'utilizzo della posta tradizionale

MESSAGGIO DA INSERIRE IN CODA A FAX
Chi riceve il presente messaggio è tenuto a verificare se lo stesso non gli sia pervenuto per errore. In tal caso è pregato di avvisare immediatamente il mittente e, tenuto conto delle responsabilità connesse all'indebito utilizzo e/o divulgazione del messaggio e/o delle informazioni in esso contenute, voglia cancellare l'originale e distruggere le varie copie o stampe.

MESSAGGIO DA INSERIRE IN CODA A E-MAIL
Chi riceve il presente messaggio è tenuto a verificare se lo stesso non gli sia pervenuto per errore. In tal caso è pregato di avvisare immediatamente il mittente e, tenuto conto delle responsabilità connesse all'indebito utilizzo e/o divulgazione del messaggio e/o delle informazioni in esso contenute, voglia cancellare l'originale e distruggere le varie copie o stampe.
I contenuti del seguente messaggio hanno valenza contrattuale esclusivamente se confermati mediante altra comunicazione effettuata mediante fax o altra comunicazione formale.

Cosa fare	Cosa non fare
Conversazioni	
	• Parlare con terzi o in luoghi pubblici o aperti al pubblico di fatti relativi all'attività aziendale • Parlare anche con colleghi o in luoghi aziendali condivisi circa informazioni alle quali tali colleghi non sono autorizzati ad accedere (compresi dati personali che non sono autorizzati a trattare)
Visitatori	
• Verificare l'identità • Invitarlo a sostare nelle aree di attesa • Accompagnarlo presso l'area di destinazione	• Lasciare documenti visibili • Consentire l'accesso alle aree riservate • Consentire l'accesso a dati o documenti • Lasciare da solo un visitatore in un locale dove sono presenti documenti
Sale riunioni	
	• Lasciare materiale nelle sale riunioni
Convegni – Pubblicazioni – Social network	
	• Dare informazioni sull'azienda e sulle attività dell'azienda senza la preventiva autorizzazione della Direzione

Trasporto all'esterno

Cosa fare	Cosa non fare
Copie di backup [*]	
• Effettuare il trasporto dei supporti dall'azienda al luogo di conservazione adottando le opportune cautele ed evitando fermate intermedie • Adottare nel luogo di conservazione i livelli di sicurezza adeguati	• Lasciare incustoditi i supporti
Documenti cartacei	
• Adottare le opportune cautele nel trasporto dei documenti, in relazione al loro contenuto (dati comuni, sensibili , giudiziari, riservati….), alla natura del documento (originale, copia…) alla rilevanza del documento (semplice, fiscale…)	• Lasciare incustoditi i documenti

[*] Attualmente non applicabile

Sicurezza fisica

Cosa fare	Cosa non fare
Accesso all'azienda	
• Rispettare l'orario di apertura e la procedura di gestione accessi	• Accedere in orari diversi da quelli indicati salvo esplicita autorizzazione • Restare in azienda soli se non autorizzati
Chiusura dell'ufficio	
La chiusura della sede è a cura del personale della Reception	
Accesso ai locali	
• Gli incaricati possono accedere ai soli locali nei quali si svolgono trattamenti per i quali sono espressamente incaricati • I locali nei quali sono conservati documenti con dati sensibili o giudiziari sono chiusi se non presidiati	

Misure antincendio

Cosa fare	Cosa non fare
• Attenersi agli specifici piani ed al regolamento aziendale • Segnalare immediatamente ai responsabili il verificarsi di situazioni di rischio	• Istruire le vie di fuga e le uscite di emergenza • Accumulare sostanze combustibili • Posizionare sostanze combustibili in luoghi non idonei • Fumare • Utilizzare prese multiple • Utilizzare apparecchiature non fornite/autorizzate dall'azienda • Utilizzare apparecchiature o prese elettriche per le quali si abbiano dubbi sul corretto funzionamento

Gestione documenti

Cosa fare	Cosa non fare
Accesso documenti cartacei	
• Accedere, anche solo in consultazione, esclusivamente ai documenti per i quali si è stati espressamente autorizzati in base al proprio ruolo • I documenti vanno prelevati dall'archivio e trattati in modo tale che terzi non autorizzati non possano accedervi • I documenti, al termine del trattamento o comunque al termine della giornata lavorativa, vanno riposti in archivio o nei propri cassetti opportunamente chiusi a chiave • I documenti con dati particolari (sensibili, giudiziari…) sono costantemente chiusi a chiave, salvo il tempo strettamente necessario al loro uso • Durante i trattamenti conservare i documenti in cartellette opache; nel caso di trattamenti di dati sensibili o giudiziari o il cui trattamento presenta rischi specifici in contenitori muniti di serratura • I documenti possono essere consegnati esclusivamente all'interessato al quale si riferiscono i dati	• Lasciare documenti incustoditi sulle scrivanie • Mostrare i documenti a terzi non autorizzati • Portare fuori dall'azienda dati o documenti se non preventivamente autorizzati • Permettere l'accesso, anche in sola consultazione, ai documenti nei locali che sono accessibili a terzi • Appendere documenti o scrivere su lavagne, informazioni contenenti dati personali in locali accessibili a terzi
Postazione di lavoro	
• Riporre tutti i documenti prima di lasciare l'ufficio	• Lasciare incustoditi i documenti • Lasciare informazioni in vista sulla scrivania o sul pc
Fotocopiatrici/Stampanti	
• La copia va trattata come l'originale • Distruggere le copie non riuscite • Trasportare originale e copia con l'adeguata cura • Cancellare la memoria	• Dimenticare l'originale • Fare copie inutili di documenti • Mostrare o distribuire copie a chi non è autorizzato al trattamento
Rifiuti	
• Verificare che i documenti con dati personali non siano recuperabili, effettuandone una preventiva distruzione • Distruggere i supporti informatici e le apparecchiature in base alle disposizioni di legge	• Gettare documenti o supporti leggibili se contengono dati personali o riservati

Cessazione del trattamento

La cessazione dei trattamenti è regolamentata dall'articolo 16 del DLgs 196/03:

In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

a) distrutti;

b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;

d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

GESTIONE DEI DIRITTI DELL'INTERESSATO

Lei deve dare pronta soddisfazione alle richieste che i soggetti interessati possono rivolgerLe, conformemente a quanto prescritto dall'articolo 7 Dlgs 196/2003 (Diritto di accesso ai dati personali ed altri diritti), segnalando tali richieste al Titolare.

Cosa fare	Cosa non fare
Gestione dei diritti dell'interessato	
• Comunicare immediatamente al Titolare o Responsabile richieste da parte di qualunque interessato	• Ignorare richieste effettuate oralmente da parte degli interessati