

# Linee guida per la gestione dei documenti informatici

Aprile 2005

## Introduzione

I documenti aziendali sono strumenti necessari ed estremamente importanti, sia da un punto di vista prettamente contenutistico che da un punto di vista legale, poiché possono costituire prove, anche in ambito giudiziale, di diritti od obblighi di un soggetto. Con il crescente affidamento creatosi sui documenti informatici è divenuto di vitale importanza per le aziende e gli enti provvedere alla revisione di eventuali policy per la gestione documentale vigenti all'interno della struttura e ciò al fine di tenere in debita considerazione le nuove modalità operative e i nuovi obblighi ad esse correlate.

Da tempo costituisce buona prassi per una azienda dotarsi di una policy per la gestione dei documenti alla cui osservanza siano tenuti non solo i dipendenti ma anche i fornitori dell'azienda ed i suoi consulenti. Questo tipo di policy (spesso denominata "policy per la conservazione dei documenti", ovvero "Document Retention Policy") ha ad oggetto l'archiviazione, il reperimento, la conservazione e la cancellazione di documenti di ogni genere.

Si tenga presente che quando si parla di "documenti" si intende far riferimento non solo alle registrazioni formali delle operazioni, come le registrazioni contabili e i contratti, ma anche alla documentazione, spesso non munita di rilevanza formale, come la corrispondenza, i memorandum interni, le e-mail e le note personali. Tali documenti possono acquisire rilevanza probatoria in ambito giudiziale e, se ancora esistenti, vi può essere l'obbligo di produrli nell'ambito di controversie legali o nel corso di indagini amministrative o regolamentari. Inoltre, si tenga presente che in ambito giudiziale, i documenti solitamente assumono rilevanza indipendentemente dal tipo di formato o supporto sul quale sono conservati (es. formato cartaceo, video, elettronico o su microfiches).

L'elaborazione di una policy per la gestione documentale necessita di un'analisi approfondita. Infatti, i dati - e i documenti oggetto di archiviazione e gestione - possono risiedere in diversi ambienti o luoghi. Per esempio, i documenti possono essere salvati su copie di back up giornaliere, settimanalmente o mensilmente; inoltre, i file contenenti i dati possono essere conservati non solo su nastro,

ma continuare a risiedere anche sull'hard disk del computer, in folder temporanei del computer, su floppy disk, su network drive o su supporti removibili. Ulteriormente i documenti informatici, gli "instant messages" e le e-mail possono avere un ambito di circolazione (e quindi di conoscenza) ben più ampio rispetto a coloro che ne sono gli effettivi destinatari. Infine, il periodo di conservazione delle informazioni elettroniche può essere più lungo di quello dei documenti cartacei semplicemente in quanto i documenti informatici occupano uno spazio minore.

Lo scopo fondamentale è creare una policy per la conservazione dei documenti che sia commercialmente praticabile nell'ambiente informatico e che tenga conto di tutti gli aspetti legali e regolamentari che possono influire sull'impresa.

Queste linee guida intendono a fornire alcune informazioni sui requisiti legali e regolamentari connessi alla gestione dei documenti informatici da un punto di vista internazionale, comunitario e nazionale.



## Requisiti internazionali

In seguito all'ampio scandalo dei documenti della Enron e della Arthur Anderson, gli organismi normatori e regolamentari internazionali hanno avviato dei processi per la regolamentazione delle società e, conseguentemente, per restituire fiducia nelle stesse.

### Sarbanes-Oxley

Benché emanato negli Stati Uniti d'America, il Sarbanes-Oxley Act del 2002 ("SOX") ha implicazioni sull'organizzazione delle imprese a livello internazionale. Tutto ciò è conseguenza del fatto che viene richiesto, alle imprese che hanno affari negli Stati Uniti d'America, di armonizzare le proprie policy per la gestione documentale con le disposizioni della SOX.

### Background

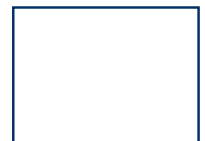
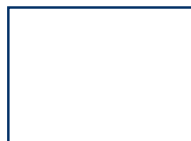
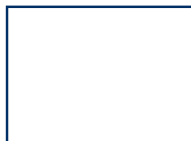
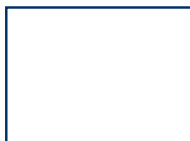
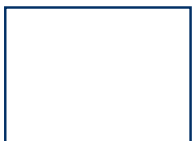
Nel dicembre 2001, la Enron fece domanda per la dichiarazione di uno dei più grandi fallimenti nella storia degli Stati Uniti d'America, ciò avvenne

quando trapelò che la Enron, a quanto si dice, aveva intrapreso numerose strategie di investimento, effettuato operazioni fuori bilancio, utilizzato società create per "mascherare" debiti, effettuato operazioni con parti correlate, ottenuto finanziamenti collaterali facendo uso di azioni proprie, effettuato inesatte, incomplete o false rappresentazioni di bilancio, fatto ricorso a metodi contabili aggressivi e a varie altre pratiche discutibili dalle quali è scaturito un ammortamento di oltre un miliardo di dollari sugli investimenti e sulle voci di guadagno correlate. Prima della domanda di fallimento presentata della Enron, i revisori contabili della stessa cominciarono a distruggere i documenti relativi alla Enron, pratica che continuò sino a che la Arthur Andersen ricevette un mandato di comparizione con il quale si ordinava di produrre quegli documenti (ormai distrutti) ed altri ancora. Come risultato la Arthur Andersen fu imputata per intralcio alla giustizia. Durante il processo il revisore contabile a capo della revisione condotta sulla Enron ammise che i documenti relativi alla compagnia elettrica erano stati distrutti.

### Dati Management e SOX

La SOX si applica alle imprese i cui titoli sono quotati o registrati presso la Securities and Exchange Commission ("SEC"). Sia le imprese statunitensi che quelle di altra nazionalità (ad esempio, società controllate da società statunitensi) possono essere soggette alla disciplina dettata dalla SOX.

Prima dell'entrata in vigore della SOX esistevano relativamente poche linee guida sulla conservazione dei dati. La SOX ha posto in evidenza tale tematica, estendendo la portata della normativa in materia di intralcio alla giustizia relativa alla conservazione dei dati e aumentando considerevolmente le sanzioni penali ad essa connesse. Conseguentemente, la SOX viene vista come il punto di riferimento per la trasparenza di una impresa. Conservazione (art. 802)  
In base alla SOX la distruzione di documenti societari "in previsione di" una "indagine federale" o di una "amministrazione di qualsiasi genere" costituisce ora reato, con sanzioni fino ad un massimo di 20 anni di reclusione e multe fino a 10 milioni di dollari per chiunque:



*"coscientemente alteri, distrugga, elimini in parte, occulti, dissimuli, falsifichi o inserisca dati falsi in registrazioni, documenti o altro materiale al fine di impedire, ostacolare o influenzare le indagini o l'adeguata amministrazione di qualsiasi materia di competenza di un dipartimento o di una agenzia degli Stati Uniti o di un procedimento avviato ai sensi del ["Bankruptcy Code", il Codice Fallimentare] ovvero in relazione a, o in previsione di, uno dei casi suddetti" (art. 802 SOX).*

#### *Comunicazione (Artt. 302 e 906)*

Oltre ai requisiti di conservazione previsti dall'art. 802, la SOX ha introdotto alcuni obblighi concernenti la comunicazione dei dati.

Ai sensi dell'art. 302 il Presidente (CEO) ed il Direttore Finanziario (CFO) di una società devono certificare personalmente *"ogni relazione annuale o trimestrale emessa"* dalla società. Essi inoltre devono fornire assicurazione sull'adeguatezza dei controlli interni relativi in materia di comunicazione di informazioni.

Come previsto dall'art. 802, rendere "coscientemente" o "volontariamente" una falsa certificazione è soggetto a sanzioni penali consistenti, rispettivamente, nella reclusione fino ad un massimo di 10 anni e/o 1 milione di dollari di multa, oppure nella reclusione sino ad un massimo di 20 anni e/o 5 milioni di dollari di multa (art. 906). In tale ipotesi la SEC può altresì avviare un procedimento in sede civile.

Queste ed altre misure legali hanno avuto l'effetto di ampliare lo scopo della conservazione e comunicazione di documenti. Le imprese dovrebbero pertanto guardare con particolare attenzione ed in un'ottica globale alle policy per la conservazione dei documenti, in particolare laddove possano esistere registrazioni non aventi carattere formale. Si possono verificare del resto casi in cui, pur in assenza di specifici obblighi legislativi e/o regolamentari che richiedano la conservazione dei documenti, risulta del tutto inammissibile la distruzione di documenti informali (per esempio, e-mail).

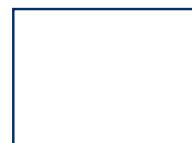
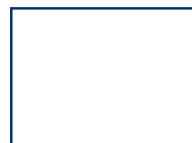
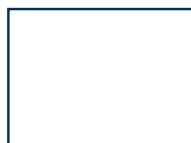
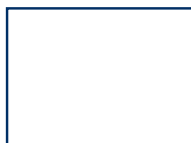
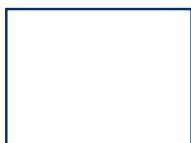
## Requisiti comunitari

### Basilea II

Per quanto riguarda l'Unione Europea, la Commissione Europea ha avanzato alcune proposte per "rilanciare" due direttive relative agli enti creditizi e alla adeguatezza patrimoniale delle imprese di investimento e degli enti creditizi (Direttiva sull'Adeguatezza Patrimoniale) al fine di realizzare Basilea II.

Basilea II è un accordo internazionale sviluppato dal Comitato di Basilea sul Controllo Bancario con l'intento di creare un nuovo standard internazionale sulle modalità di valutazione e distribuzione del rischio da parte di banche e altri istituti finanziari. Alla stessa stregua della SOX, Basilea II mira ad aumentare la trasparenza delle banche e degli istituti finanziari ampliandone gli obblighi di comunicazione.

Basilea II si fonda su tre pilastri (chiamati "obiettivi"), che si rinforzano vicendevolmente, studiati per assicurare la sicurezza e la stabilità dei sistemi finanziari. Il 3° Pilastro (Disciplina di Mercato) definisce la struttura relativa alle comunicazioni al



mercato alle quali sono tenute le banche e gli istituti finanziari. In particolare, Basilea II impone alle imprese di effettuare comunicazioni al mercato al fine di migliorare il controllo del mercato stesso. Tali comunicazioni riguardano anche informazioni estremamente importanti sul rischio sopportato da un'impresa, i suoi processi di gestione del rischio (risk management) e l'adeguatezza del suo capitale. La comunicazione è dovuta ogni sei mesi.

Vi è perciò il rischio che una inadeguata gestione dei dati - come si verifica nel caso in cui un'impresa non sia in grado di conformarsi ai requisiti richiesti dalla suddetta direttiva - possa rendere dubbia la posizione finanziaria di una banca o di un istituto finanziario.

Si prevede che la Direttiva sull'Adeguatezza Patrimoniale venga approvata dall'Unione Europea entro l'estate 2005 e, verosimilmente, che entro la fine del 2006 gli Stati membri la rendano applicabile a livello nazionale (e, quindi, che entro tale data le imprese si siano adeguate ad essa). Resta pertanto poco tempo prima che le imprese siano tenute ad adeguarsi alla nuova normativa.

### **Direttiva sulla protezione dei dati personali**

La direttiva europea sulla protezione dei dati personali prevede alcuni obblighi ai quali una impresa è tenuta quando tratta dati personali. Per dati personali si intendono le informazioni relative alle persone fisiche, non solo nella loro sfera privata, ma anche in ambito lavorativo.

Con riferimento ai dati elettronici, un'impresa che opera in ambito comunitario deve perciò conformarsi alla disciplina sulla protezione dei dati nei limiti in cui tali documenti informatici (per esempio, e-mail) contengano informazioni personali.

L'articolo 17(1) della direttiva sulla protezione dei dati prevede l'obbligo per un'impresa di:

"adottare misure tecniche e organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di

dati personali."

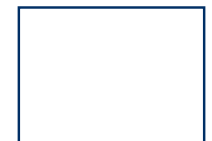
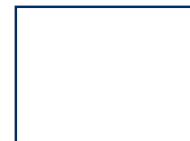
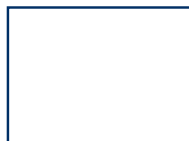
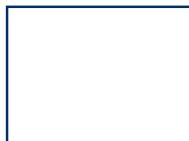
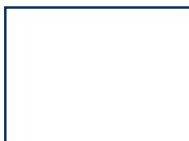
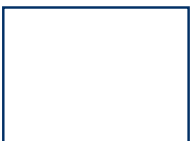
In altre parole la normativa prevede che una impresa sia tenuta per legge a mantenere buone policy e prassi interne in materia di sicurezza e di gestione dei processi informativi.

Inoltre, l'articolo 12 prevede che una impresa debba garantire ad ogni individuo il diritto di ottenere, ad intervalli ragionevoli e senza ritardi o spese eccessivi, informazioni relative al trattamento, o alla comunicazione, di dati personali che lo riguardano.

Pertanto, in tutto il territorio dell'Unione Europea gli interessati hanno il diritto di accedere alle informazioni personali, ivi incluse le e-mail, senza alcun riguardo (in senso ampio) all'eventuale disturbo che tale accesso possa arrecare all'impresa.

### **Requisiti Italiani**

Nel definire i contenuti di una policy di gestione dei documenti informatici, efficiente anche dal punto di vista commerciale e di gestione dell'azienda, non si potrà naturalmente fare a meno di individuare i requisiti legali a cui una



organizzazione aziendale è tenuta sulla base della normativa nazionale applicabile.

### *Obblighi di tenuta dei documenti*

In generale, affinché un documento informatico possa essere munito di rilevanza giuridica, ed essere utilizzato anche a fini probatori (per esempio a fini di revisione contabile, di accertamento fiscale o amministrativo o ancora nell'ambito di procedimenti giudiziari o stragiudiziali), lo stesso dovrà essere creato e conservato secondo modalità tecniche predefinite dalla normativa vigente (*T.U. in materia di documentazione amministrativa, DPR 445/2000 e regolamenti di attuazione, es. D.M 23/01/2004 in materia di tenuta dei libri contabili in formato elettronico*). Si avverte che è in fase di pubblicazione sulla G.U. il Codice dell'Amministrazione Digitale che abrogherà gran parte delle norme previste dal DPR 445/2000: per quanto qui di rilievo si precisa che la nuova normativa sarà sostanzialmente conforme a quanto previsto dal vigente DPR 445/2000). Per esempio, i documenti contabili, quelli contenenti obbligazioni contrattuali o comprovanti controversie legali devono essere conservati con modalità tali da poter essere utilizzati anche in

ambito giudiziario o per verifiche fiscali-amministrative. La legge può imporre inoltre modalità e termini minimi di conservazione per alcune tipologie di documenti informatici.

Ulteriormente, ai fini della stesura di una policy di tale genere si deve tenere conto del fatto che la tenuta ed archiviazione dei documenti elettronici è soggetta, tra l'altro, ai limiti imposti dalla normativa in materia di protezione dei dati personali (*Codice in materia di protezione dei dati personali, D.Lgs. 196/2003 e relativa normativa di attuazione, es. codici deontologici*). Si noti che, a differenza che in altri Stati della UE, la disciplina italiana sul trattamento dei dati personali trova applicazione anche con riguardo ai dati delle persone giuridiche, enti e associazioni): le modalità di raccolta, tenuta e conservazione dei documenti informatici devono essere tali da assicurare che il trattamento dei dati personali in essi contenuti sia limitato a quanto strettamente necessario per il raggiungimento delle finalità per le quali tali dati sono raccolti.

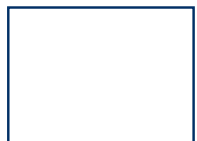
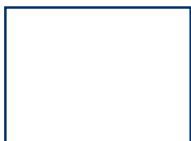
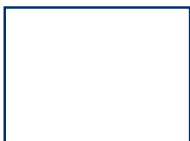
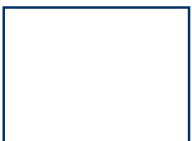
Fermo restando che le aziende sono tenute a conservare alcuni documenti in formato cartaceo (ad es., libri sociali, registro infortuni), la legge può richiedere la conservazione in formato

elettronico (ad es., registrazioni nel settore finanziario) o consentire, alternativamente al formato cartaceo, la conservazione di alcuni documenti in formato elettronico.

Per esempio, le società devono provvedere alla registrazione delle scritture contabili (es. libri contabili e corrispondenza), secondo la tempistica prevista dalla legge per ciascuna tipologia di documento (es. *artt. 2216-2217 c.c., DPR 600/73*), ed alla conservazione delle stesse per almeno 10 anni dalla relativa data, per la corrispondenza e documenti, ovvero dall'ultima registrazione, per i libri contabili (*art. 2220 c.c.*).

Inoltre i tempi di conservazione possono variare a seconda della normativa applicabile (civile o fiscale). Ad esempio, le scritture contabili devono essere conservate a fini fiscali fino alla definizione degli accertamenti relativi ai corrispondenti periodi di imposta (usualmente 5 anni, ovvero per ulteriori 2 anni dopo la scadenza del termine ordinario se non ci si è avvalsi di eventuali sanatorie, ai sensi del *DPR 600/73*).

Quanto alla documentazione informatica relativa ai rapporti di lavoro, ciascuna azienda è tenuta, in particolare, alla conservazione del



libro matricola e del libro paga, aggiornati con cadenza giornaliera (Circ. INAIL 23/3/1995 n. 17), per un periodo di 10 anni dall'ultima annotazione (DPR 1124/65, L. 12/79).

Altre restrizioni possono derivare da normativa volta all'accertamento ed alla repressione di reati: per esempio, i fornitori di servizi di telefonia sono tenuti alla conservazione dei dati di traffico telefonico per 2 anni dalla loro raccolta e, ai soli fini di accertamento e repressione di reati di particolare gravità, ivi inclusi quelli informatici e telematici, per ulteriori 2 anni (D.Lgs. 196/2003).

Obblighi di conservazione di documenti e dati informatici possono altresì derivare dalla normativa legislativa e regolamentare di settore (es. bancario, assicurativo, finanziario). Esemplicativamente, gli intermediari finanziari sono tenuti alla registrazione su supporto elettronico degli ordini impartiti dagli investitori e alla loro conservazione per almeno 8 anni, mentre la conservazione dei contratti, della corrispondenza e della relativa documentazione devono essere conservati per almeno 5 anni dalla cessazione del rapporto

contrattuale (Regolamento Consob n. 11522/98).

In alcuni casi, nonostante la legge non preveda l'archiviazione o comunque la registrazione di informazioni e/o documenti, è opportuno comunque che le aziende adottino una organizzazione tale da assicurare la conservazione di tutta quella documentazione che possa rivelarsi utile ai fini commerciali o in vista di eventuali controversie. In certi casi, infatti, diventa essenziale per una azienda, da un lato, fondare alcune delle proprie decisioni commerciali su informazioni che non necessariamente rientrano tra la documentazione di cui il legislatore nazionale ha previsto la registrazione obbligatoria e, dall'altro, conservare i documenti utili ai fini di eventuali controversie sino alla scadenza del periodo di prescrizione dei relativi diritti (in generale, 10 anni in caso di diritti derivanti da un contratto e 5 anni in caso di diritto al risarcimento del danno derivante da fatto illecito).

Si tenga infine presente che, nonostante i tempi di conservazione previsti dalla legge, qualora - in pendenza di tale termine - sia insorta

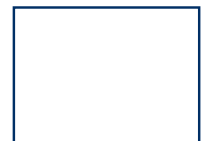
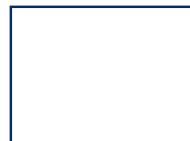
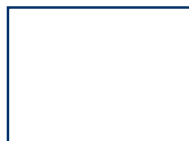
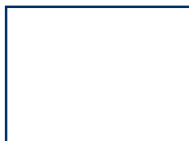
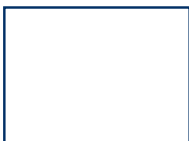
una controversia, sarà opportuno che l'azienda valuti attentamente la rilevanza di tutti i documenti in suo possesso e provveda alla conservazione degli stessi sino alla conclusione della controversia.

#### Caso 1 -Rapporti con la clientela

Un contratto può dirsi concluso con mezzi informatici quando l'utente che ha inviato via e-mail una proposta di contratto riceve dal destinatario conferma ed accettazione (se del caso, via e-mail) della relativa proposta. La relativa documentazione dovrà pertanto essere conservata per almeno 10 anni.

#### Registrazione (Archiviazione) e Aggiornamento

Come già accennato, spesso la normativa che impone obblighi di conservazione di dati e documenti prevede una disciplina specifica anche in relazione ai tempi entro cui le relative registrazioni devono avvenire e alle modalità con cui le stesse devono essere effettuate (es. le registrazioni degli ordini di strumenti finanziari devono essere effettuate entro il giorno successivo a quello di



ricezione ed essere tali da consentire in qualsiasi momento di effettuare ricerche ed estrazioni secondo criteri di ricerca predefiniti).

Un principio generale in tema di registrazione ed aggiornamento dei documenti si evince in ogni caso dalla normativa in materia di protezione dei dati personali la quale impone che i dati personali raccolti e registrati da una azienda (es. dati del personale, ivi incluse e-mail, dati dei clienti e dei fornitori), oltre ad essere stati raccolti lecitamente, devono essere sempre esatti, completi ed aggiornati (eventualmente su richiesta dello stesso interessato). L'azienda dovrà pertanto adottare procedure tali da assicurare il rispetto di tale principio, anche mediante l'adozione delle misure di sicurezza imposte dalla normativa (*D.Lgs. 196/2003*).

#### Caso 2 -Qualità e integrità documenti

Ciascun aggiornamento o modifica dei documenti informatici, se consentito, dovrà essere registrato e datato. Ulteriormente dovrà adottarsi una procedura periodica di controllo dell'integrità dei dati/documenti.

#### Accesso e Comunicazione

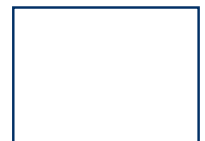
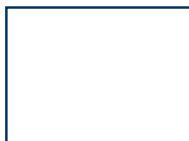
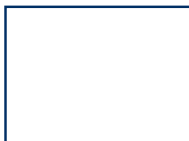
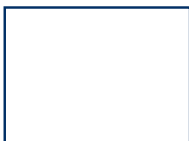
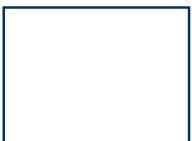
Una volta registrati i documenti devono poter essere accessibili secondo le esigenze organizzative e commerciali dell'azienda, ma anche nel rispetto della normativa applicabile.

In particolare, a pena di sanzioni anche penali, l'azienda è tenuta ad adottare misure di sicurezza tali da assicurare che l'accesso alla documentazione sia garantito, secondo precise regole interne, solo al personale dalla stessa appositamente autorizzato e che ai documenti informatici non abbiano accesso terzi estranei alla stessa, salvo nei casi previsti dalla legge (es. enti che controllano la tenuta dei libri matricola e paga, Guardia di Finanza, revisori dei conti, ecc.) o altrimenti autorizzati dall'azienda o dall'interessato, in caso di dati personali (es. consulente del lavoro) (*D.Lgs. 196/2003*).

L'azienda deve altresì adottare misure tali da garantire che i singoli individui (anche persone giuridiche) possano esercitare il proprio diritto di conoscere se l'azienda detiene e tratta informazioni che li riguardano e di ottenere, per esempio, il loro aggiornamento, rettifica o, se del caso, la cancellazione.

Come accennato, le policy in materia devono anche prevedere modalità tali da garantire la conservazione della documentazione utile in caso di eventuali controversie e la loro facile individuabilità ed accessibilità in tale ipotesi. E' infatti possibile che nell'ambito di un procedimento un'azienda abbia diritto di accedere a, o sia tenuta a rendere accessibile alla controparte, documenti informatici rilevanti ai fini del procedimento stesso (es. ordine di esibizione, sequestro).

Il documento informatico può infatti essere utilizzato quale prova nell'ambito di un procedimento, giudiziale o stragiudiziale (*artt. 2702 e segg. c.c., DPR 445/2000*). L'efficacia probatoria del documento informatico varia in funzione dei requisiti tecnici con i quali è stato creato o conservato, arrivando addirittura a dare prova della autenticità del documento (provando che lo stesso proviene da un certo soggetto) e della data dello stesso (marca temporale). I documenti informatici potranno infatti valere quali semplici riproduzioni meccaniche - e quindi fornire prova di un fatto salvo che la loro conformità ai fatti rappresentati sia disconosciuta dalla controparte (*art 2712 c.c.*) - o



addirittura quale scrittura privata (in caso di apposizione di firma digitale) così dando prova, fino a querela di falso, della provenienza di un documento da un certo soggetto e della relativa data (*artt. 2702 e 2704 c.c.*).

Caso 3 - Valore probatorio delle e-mail  
Negli USA, ad esempio, alcuni giudici hanno mostrato di basare le proprie decisioni su alcune e-mail rinvenute all'interno di computer aziendali che erano stati sequestrati (ciò è accaduto, in particolare, in uno dei procedimenti a carico di Microsoft per abuso di posizione dominante). Anche in Italia di recente, alcuni giudici hanno fondato l'accoglimento di alcune richieste di emissione di decreti ingiuntivi sulla base di dichiarazioni di riconoscimento di debito contenute in e-mail inviate dal debitore al proprio creditore (Trib. Cuneo 15/12/2003 (decr.ing. n. 848), Trib. Mondovì 7/6/2004 (decr. ing. n. 375)).

Non si dimentichi, infine, che i documenti informatici possono essere oggetto di specifici diritti di accesso, come nel caso dei dati, documenti e procedure della pubblica amministrazione in relazione ai quali vige un generale diritto di accesso dei privati a tali informazioni (art. 59 DPR 445/2000).

### *Accesso e Concorrenza*

Si sottolinea, infine, che con provvedimento n. 8545 del 27 luglio 2000, anche società terze che intendono fornire i servizi di informazione abbonati hanno ottenuto, con disposizione dell'Autorità Garante della Concorrenza e del Mercato, la cessione gratuita da parte di Telecom dell'intero data base degli abbonati al servizio telefonico. Il fatto che un'azienda possa essere tenuta alla esibizione, o addirittura alla cessione, di documenti informatici a terzi in presenza di specifici ordini o provvedimenti emessi da autorità competenti (es. AGCOM), rileva un ulteriore aspetto, ovvero che la creazione di data base informatici può essere rilevante anche ai fini della concorrenza.

### *Distruzione e manipolazione*

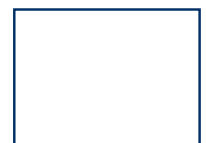
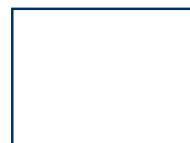
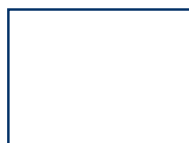
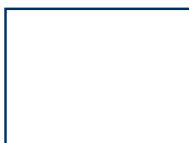
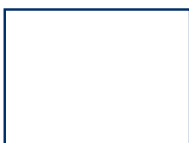
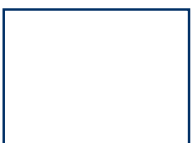
Le aziende devono essere consapevoli che quando sussistono obblighi di conservazione dei documenti informatici, la distruzione, anche accidentale, di tali documenti prima della scadenza del termine di conservazione può essere causa di sanzioni. Si pensi ad esempio al caso di distruzione di documenti contabili che

espone gli amministratori della società al rischio di sanzioni amministrative e/o penali per impedito controllo ai soci o per irregolare/omessa conservazione dei libri contabili (*libro V, tit. XI, c.c.*).

Ulteriormente, le aziende sono tenute ad adottare misure di sicurezza tali da evitare che i documenti informatici vengano impropriamente manipolati o illegittimamente modificati. Si pensi, ad esempio, al caso di falsificazione di documentazione contabile che espone gli organi della società a possibili sanzioni penali (*art. 2638 c.c.*).

Quando infine le aziende non sono più tenute alla conservazione dei documenti, le stesse possono trovarsi in una delle due seguenti situazioni:

- a) obbligo di distruggere i documenti: al di fuori di un generico obbligo, facente capo a tutte le aziende (in quanto titolari del trattamento), di distruzione/cancellazione dei dati personali non più necessari al raggiungimento degli scopi per i quali gli stessi sono stati raccolti (*D.Lgs. 196/03*), la legge può a volte dettare regole specifiche in tema di termine massimo di



conservazione dei dati. Ad esempio, i fornitori di servizi di comunicazione elettronica devono cancellare immediatamente i dati di traffico non più necessari per la trasmissione della comunicazione, o - se necessari per la fatturazione - dopo un periodo massimo di 6 mesi, fatto salvo il caso di eventuali contestazioni giudiziali; altri termini di conservazione sono imposti a coloro che gestiscono centrali rischi private (*Deliberazione del Garante per la protezione dei dati personali, n. 8 del 16 /11/2004*);

b) possibilità di conservare ulteriormente i documenti in presenza di ragioni organizzative ed aziendali, purché compatibili con le norme in materia di protezione dei dati personali (ad es. la azienda può scegliere di conservare i documenti rendendo anonimi i dati personali da essa detenuti).

Naturalmente le policy in materia di gestione dei documenti informatici deve tenere in considerazione numerosi fattori, ivi incluse le esigenze di spazio per l'archiviazione ed i costi ad essa connessi, l'importanza per

l'azienda di avere la disponibilità di certi documenti in futuro (e ciò anche alla luce dell'eventuale danno che potrebbe derivare alla stessa in caso di distruzione degli stessi). Tali considerazioni devono essere rimesse alle valutazioni non solo del management dell'azienda, ma anche della persona deputata alla valutazione dei rischi.

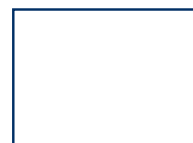
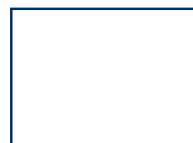
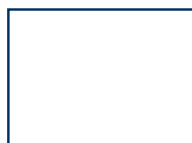
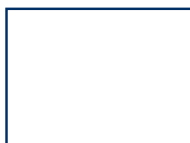
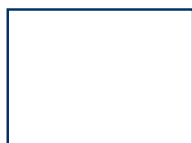
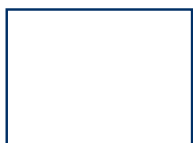
Risulta pertanto importante che, al fine di aumentare la propria efficienza, l'azienda individui al suo interno uno o più soggetti (in funzione della propria struttura organizzativa) responsabili per la realizzazione effettiva e giornaliera della policy. Inoltre, ai diversi responsabili, così come selezionati dall'azienda dovrebbe essere data la possibilità di confrontarsi sulle diverse conoscenze acquisite in ciascun ambito lavorativo ricordando che la cancellazione e distruzione dei documenti e dei relativi dati deve essere effettuata in modo da garantire la completa eliminazione di qualsiasi traccia di tali dati dai supporti informatici, provvedendo - nel caso di supporti rimovibili e laddove necessario (es. nel caso di dati sensibili) - anche alla eventuale distruzione di tali supporti o a rendere gli stessi inutilizzabili.

#### Caso 4 - Cosa dice di te il tuo computer?

Nell'ambito di una recente ricerca, alcuni ricercatori universitari hanno scoperto che dati aziendali e informazioni personali sensibili non erano state rimosse, prima della loro vendita, da computer di seconda mano. Dati identificativi dei precedente proprietari sono stati rinvenuti sul 50% degli apparecchi ed il 20% degli apparecchi conteneva informazioni finanziarie. Solo due dei novanta computer esaminati non contenevano dati recuperabili.

#### Bird & Bird

Bird & Bird è uno studio legale commerciale internazionale che unisce una professionalità legale all'avanguardia ad una conoscenza approfondita di settori industriali fondamentali: information technology, e-commerce, comunicazioni, bioscienze, media, sport, settore aeronautico, servizi bancari e finanziari. Siamo orgogliosi di lavorare con alcune delle società più innovative e tecnologicamente avanzate del mondo, ciascuna delle quali conta su una consulenza legale all'avanguardia



per la realizzazione dei propri obiettivi di business.

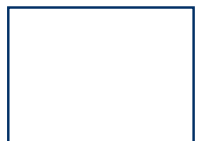
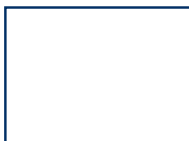
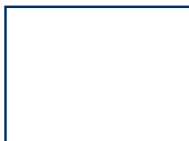
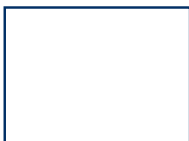
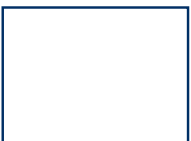
Con sedi in Europa, Cina e Hong Kong e con stretti collegamenti con studi legali situati nel resto del mondo, siamo in una posizione favorevole per offrire ai nostri clienti competenza locale in un contesto internazionale. I professionisti di ciascuno dei nostri studi lavorano a stretto contatto per fornire un servizio internazionale personalizzato basato sulle specifiche esigenze del cliente. Ogni studio è composto da professionisti locali dotati di una grande capacità di comprensione delle condizioni economiche e culturali locali abbinata ad una profonda conoscenza dei settori e delle aree legali in cui sono specializzati.

all'hardware e alla manodopera. Con un fatturato di 2,04 miliardi di dollari nel 2004, VERITAS fornisce prodotti e servizi per la protezione dei dati, archiviazione e gestione dei server, oltre a software high availability e gestione delle performance degli applicativi, utilizzati dal 99 % delle società Fortune 500.

Maggiori informazioni su VERITAS Software possono essere trovate sul sito [www.veritas.com](http://www.veritas.com).

## VERITAS Software

VERITAS Software, una delle 10 più grandi società di software al mondo, è uno dei più importanti fornitori di software e di servizi per la creazione di infrastrutture di utility computing. In un modello di utility computing le risorse IT sono allineate con le esigenze commerciali e gli applicativi di business sono forniti con performance e disponibilità ottimali in aggiunta a infrastrutture condivise, minimizzando i costi connessi



---

# BIRD & BIRD

[www.twobirds.com](http://www.twobirds.com)

---

## Beijing

---

3614, China World Trade  
Centre, Tower 1  
1 Jianguomenwai Dajie  
Chaoyang District  
Beijing 100004  
PRC  
Tel: +86 10 6505 6667  
Fax: +86 10 6505 9469

---

## Brussels

---

Avenue d'Auderghem 22-28  
1040 Brussels  
Belgium  
Tel: +32 (0)2 282 6000  
Fax: +32 (0)2 282 6011

---

## Düsseldorf

---

Karl-Theodor-Strasse 6  
D 40213 Düsseldorf  
Germany  
Tel: +49 (0)211 2005 6000  
Fax: +49 (0)211 2005 6011

---

## The Hague

---

Parkstraat 31  
2514 JD The Hague  
P.O. Box 30311  
2500 GH The Hague  
The Netherlands  
Tel: +31 (0)70 353 8800  
Fax: +31 (0)70 353 8811

---

## Hong Kong

---

6/F ICBC Tower  
Citibank Plaza  
3 Garden Road  
Hong Kong  
Tel: +852 2248 6000  
Fax: +852 2248 6011

---

## London

---

90 Fetter Lane  
London  
EC4A 1JP  
UK  
Tel: +44 (0)20 7415 6000  
Fax: +44 (0)20 7415 6111

---

## Milan

---

Via Montenapoleone, 10  
20121 Milan  
Italy  
Tel: +39 02 30 35 6000  
Fax: +39 02 30 35 6011

---

## Munich

---

Pacellistrasse 14  
80333 Munich  
Germany  
Tel: +49 (0)89 3581 6000  
Fax: +49 (0)89 3581 6011

---

## Paris

---

Centre d'Affaires  
Edouard VII  
3 square Edouard VII  
75009 Paris  
France  
Tel: +33 (0)1 42 68 6000  
Fax: +33 (0)1 42 68 6011

---

## Stockholm

---

Norrandsgatan 15  
Box 7714  
SE-103 95 Stockholm  
Sweden  
Tel: +46 (0)8 506 320 00  
Fax: +46 (0)8 506 320 90

---