

# 1-Premessa

## 1.1 GLI ADEMPIMENTI

Dal 1° gennaio 2004 è in vigore il nuovo "Codice in materia di protezione dei dati personali" (d.lgs. 196/2003) che costituisce una raccolta sistematica di tutte le disposizioni normative in materia di privacy.

La disciplina in esso contenuta si applica a chiunque faccia trattamento di dati personali.

Il T.U. distingue tre categorie di dati: i dati comuni (nome, cognome, telefono, fax, codice fiscale, partita Iva, etc.); i dati sensibili (dati idonei a rilevare origine razziale, convinzioni religiose, opinioni politiche, stato di salute, vita sessuale, etc.) e i dati giudiziari (dati relativi al casellario giudiziale, qualità di imputato o indagato).

Tutte le aziende, i professionisti, le associazioni e le amministrazioni pubbliche (ovvero chiunque tratti dati personali di clienti, fornitori, pazienti, associati ecc..) sono pertanto assoggettati dal nuovo Codice ad una serie di adempimenti. Molti di essi, peraltro, erano già previsti dalla precedente normativa in materia, ma nel nuovo Codice sono stati variamente modificati.

Gli obblighi sono differenziati a seconda della tipologia dei dati trattati, delle modalità del trattamento e dall'esistenza o meno di una struttura informatica.

**Gli unici ad esserne dispensati (Art. 5 comma 3) sono le persone fisiche in caso di trattamento a fini esclusivamente personali a condizione che i dati non vengano diffusi, ferma restando la responsabilità civile (Art. 15) e gli obblighi di sicurezza (Art .31).**

## 1.2 L'INFORMATIVA

Invariato rimane l'obbligo di rendere adeguata informativa all'interessato al trattamento dei dati, ossia alla persona, fisica o giuridica, alla quale i dati si riferiscono.

L'art. 13 del nuovo Codice impone al titolare del trattamento di dati personali (ossia l'azienda nel suo complesso) l'obbligo di informare preventivamente l'interessato sugli elementi essenziali del trattamento.

Rispetto alla precedente normativa è ora previsto che debbano essere espressamente indicati nell'informativa tutti i soggetti ai quali i dati potranno essere comunicati, per il resto l'impianto dell'informativa è sostanzialmente invariato.

Per quanto riguarda il consenso, va detto che non è più necessario acquisirlo nei casi in cui il trattamento dei dati è necessario per adempiere un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria oppure è necessario per eseguire gli obblighi derivanti da un rapporto contrattuale tra le parti.

Mentre rimane senz'altro l'obbligo di acquisire il consenso espresso e scritto nel caso in cui i dati possano essere utilizzati per compiere ricerche di mercato o per l'invio di materiale pubblicitario e nel caso di trattamento di dati sensibili, ossia di dati 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 sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

### **1.3 LA NOTIFICA AL GARANTE**

La notifica consiste nella comunicazione che l'azienda, il professionista o la pubblica amministrazione devono inoltrare al Garante al fine di segnalare le tipologie e le modalità di trattamento dei dati che intende effettuare.

In base al nuovo Codice hanno l'obbligo di eseguire la notificazione soltanto i titolari che effettuano i trattamenti espressamente elencati al 1° comma dell'art. 37:

- \* dati genetici, biometrici o dati che indicano la posizione geografica di persone o oggetti mediante una rete di comunicazione elettronica;
- \* dati idonei a rivelare lo stato di salute e la vita sessuale trattati ai fini di procreazione assistita, prestazione di servizi sanitari, indagini epidemiologiche, rilevazioni di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- \* dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti ed organismi senza scopo di lucro a carattere politico, filosofico, religioso o sindacale;
- \* dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato o ad analizzare abitudini o scelte di consumo o monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi;
- \* dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- \* dati registrati in apposite banche dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti e fraudolenti.

### **1.4 CONSERVAZIONE E COMUNICAZIONE E DIFFUSIONE**

I dati personali vanno conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e trattati. Tali dati possono essere comunicati e diffusi nei limiti strettamente pertinenti all'espletamento dell'incarico conferito.

### **1.5 I SOGGETTI CHE EFFETTUANO IL TRATTAMENTO**

All'interno di ogni azienda si dovrà provvedere, laddove non si sia già effettuato, all'individuazione di tre soggetti:

- il titolare del trattamento: persona fisica o ente nel suo complesso in caso di società.
- il responsabile del trattamento: figura facoltativa designata dal titolare e predisposta a verificare i corretti adempimenti di legge.
- gli incaricati del trattamento: ovvero le persone fisiche autorizzate a compiere operazioni di trattamento, nel caso di specie tutti i "collaboratori" dell'azienda (impiegati etc.).

## **1.6 DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

Per i titolari di un trattamento di dati sensibili o di dati giudiziari effettuato mediante l'uso di strumenti elettronici il nuovo Codice prevede l'obbligo di redigere entro il 31 marzo di ciascun anno un documento programmatico sulla sicurezza che deve contenere le informazioni di cui al punto 19 del disciplinare tecnico in materia di misure di sicurezza (allegato B del Codice).

Al punto 26 del disciplinare tecnico (allegato B del Codice) è altresì previsto che il titolare del trattamento riferisca, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

## **1.7 MISURE MINIME DI SICUREZZA**

Occorre premettere che per chiunque tratti dati personali vale il principio generale stabilito dall'art. 31 del Codice in base al quale i dati personali devono essere custoditi e controllati in modo da contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.

Il Codice prevede poi alcune misure indispensabili, le cosiddette "misure minime" in modo che sia assicurato un livello minimo di protezione dei dati personali.

Tali misure differiscono a seconda del tipo di trattamento effettuato dal titolare e dal tipo di dato trattato.

### **1.7.1 MISURE MINIME CHE DEVONO ESSERE ADOTTATE DALLE IMPRESE CHE TRATTANO DATI PERSONALI SOLO CON STRUMENTI CARTACEI**

- \* Dare lettera di incarico ai dipendenti per i trattamenti consentiti;
- \* Verificare, annualmente, gli incarichi affidati ai dipendenti;
- \* Conservare gli atti e i documenti in armadi chiusi e seguire una procedura in base alla quale tali atti e documenti sono affidati alla custodia degli incaricati solo per il tempo necessario allo svolgimento dei relativi compiti.

### **1.7.2 MISURE MINIME CHE DEVONO ESSERE ADOTTATE DALLE IMPRESE CHE TRATTANO DATI PERSONALI SOLO CON STRUMENTI ELETTRONICI**

- \* Dare lettere di incarico ai dipendenti per i trattamenti consentiti;
- \* Provvedere al periodico aggiornamento (con cadenza almeno annuale) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- \* Disporre di un sistema di autenticazione informatica. Questo nel senso che ad ogni incaricato che effettua trattamento di dati personali con strumenti elettronici dovrà corrispondere un codice per l'identificazione (user name) dell'incaricato associato ad una parola chiave riservata (password) conosciuta solamente dal medesimo. Il codice prevede che in alternativa possano essere utilizzati anche altri sistemi di autenticazione ma di più difficile adozione (token/smart-card/caratteristiche biometriche dell'incaricato eventualmente associate ad un codice identificativo o a una parola chiave);
- \* Proteggere i dati personali contro il rischio di intrusione e dell'azione di programmi di cui all'art 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale (antivirus);

\* Provvedere almeno annualmente all'aggiornamento periodico dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti (programmi patch: letteralmente "pezze", in pratica aggiustamenti che le case produttrici di software creano per risolvere bug o problemi al software non riscontrati in fase di test).

Nel caso di trattamenti di dati sensibili o giudiziari l'aggiornamento delle patch è almeno semestrale;

\* impartire istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale (back-up).

## **1.8 LE SANZIONI**

### **1.8.1 ILLECITI CIVILI**

L'art. 15 ribadisce il carattere di attività pericolosa del trattamento dei dati personali: "chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile".

Il titolare per evitare di risarcire il danno dovrà dimostrare di aver adottato tutte le misure idonee ad evitare il verificarsi del danno.

### **1.8.2 ILLECITI AMMINISTRATIVI E PENALI**

Il Codice prevede un generale inasprimento delle sanzioni. In particolare: chi omette di adottare le misure minime di sicurezza è punito con l'arresto fino a due anni o con l'ammenda da diecimila a cinquantamila euro.

"Ulteriori misure minime devono essere adottate dalle Imprese che trattano dati personali sensibili o giudiziari con strumenti elettronici (firewall o similari, "distruzione" supporti rimovibili, ecc.)"

## 2-OPERAZIONI

### 2.1 IL TITOLARE DEL TRATTAMENTO

Occorre individuare il titolare del trattamento, ovvero la persona fisica o ente nel suo complesso in caso di società, ed inserire i suoi dati nella schermata del programma associata al pulsante "Titolare del Trattamento", ignorando per il momento i campi relativi a Responsabile, Amministratore di sistema e Custode dei codici di accesso. In questa versione del programma non è prevista la presenza di più contitolari, quindi non è possibile inserire più record di tipo Titolare.

DL196/AV Ver.1.1 del 25.11.2005 [Titolare del Trattamento]

Principale

Titolare del Trattamento

Vedemecum

Adempimenti

Risorse

Locali

Uscita

Inserimento Dati

Stampe

Strumenti

**Ragione Sociale**  
AGENZIA VIAGGI

Indirizzo  
Via

CAP Comune Provincia  
66034 LANCIANO CH

Codice Fiscale

Partita IVA  
01234567893

Responsabile del trattamento  
MAURIZIO AMOROSO

Amministratore di sistema  
MAURIZIO AMOROSO

Custode dei codici di accesso  
MAURIZIO AMOROSO

Programma realizzato da  
Italo Amoroso & Federico Violante  
distribuito con metodo  
"shareware"  
da Maurizio Amoroso

Gli autori non rispondono  
e declinano  
ogni responsabilità diretta o  
indiretta per le perdite,  
i mancati guadagni,  
ed i danni che possono derivare  
dall'utilizzo della procedura.

Tutti i diritti sono di proprietà  
degli autori

## 2.2 LE RISORSE UMANE

Occorre ora inserire i dati delle risorse umane coinvolte a qualsiasi titolo, nel trattamento dei dati. Le risorse umane presumibilmente saranno più una. Per inserire nuovi record occorre cliccare sul terzo pulsantino in alto, quello con il simbolo “+”. Il pulsantino a fianco, con il simbolo della matita consente la modifica del record. La modalità di modifica viene implicitamente attivata cliccando su un campo e iniziando a digitare. Cliccando sul pulsante con il simbolo del Floppy o selezionando un'altra schermata i dati vengono salvati. Per annullare la modifica cliccare sul pulsante con la croce nera.

Il penultimo pulsante, quello con la crocina rossa permette di annullare mentre il terz'ultimo attiva la modalità di ricerca. Quando i pulsanti sono grigi, la loro funzionalità non è attiva in quel contesto.

DL196/AV Ver.1.1 del 25.11.2005[Risorse]

Principale

Titolare del Trattamento

Vedemecum

Adempimenti

Risorse

Locali

Uscita

Inserimento Dati

Stampe

Strumenti

**Nominativo**

MAURIZIO AMOROSO

Nato il  
03/02/1957

Nato a  
LANCIANO

Prov.  
CH

Codice Fiscale  
MRSMRZ57B03E435S

Tipo di rapporto  
titolare/amministratore

I tipi di rapporto sono definiti in una tabella di sistema e non possono essere modificati in questa versione del programma. In ogni caso nessun utente al momento ha segnalato la necessità di ridefinirli.

The screenshot shows a software window titled "DL196/AV Ver.1.1 del 25.11.2005 [Risorse]:Modifica". The interface includes a sidebar with navigation icons for "Principale", "Titolare del Trattamento", "Vedemecum", "Adempimenti", "Risorse", "Locali", and "Uscita". The main area contains a form with the following fields:

- Nominativo: MAURIZIO AMOROSO
- Nato il: 03/02/1957
- Nato a: LANCIANO, Prov.: CH
- Codice Fiscale: MRSMRZ57B03E435S
- Tipo di rapporto: A dropdown menu is open, showing options: titolare/amministratore (highlighted), collaboratore esterno, dipendente, praticante, professionista, società terza, and titolare/amministratore.

At the bottom of the sidebar, there are buttons for "Inserimento Dati", "Stampe", and "Strumenti".

Inserire i dati di **tutti** i soggetti coinvolti, che in seguito saranno identificati come responsabili e/o incaricati del trattamento.

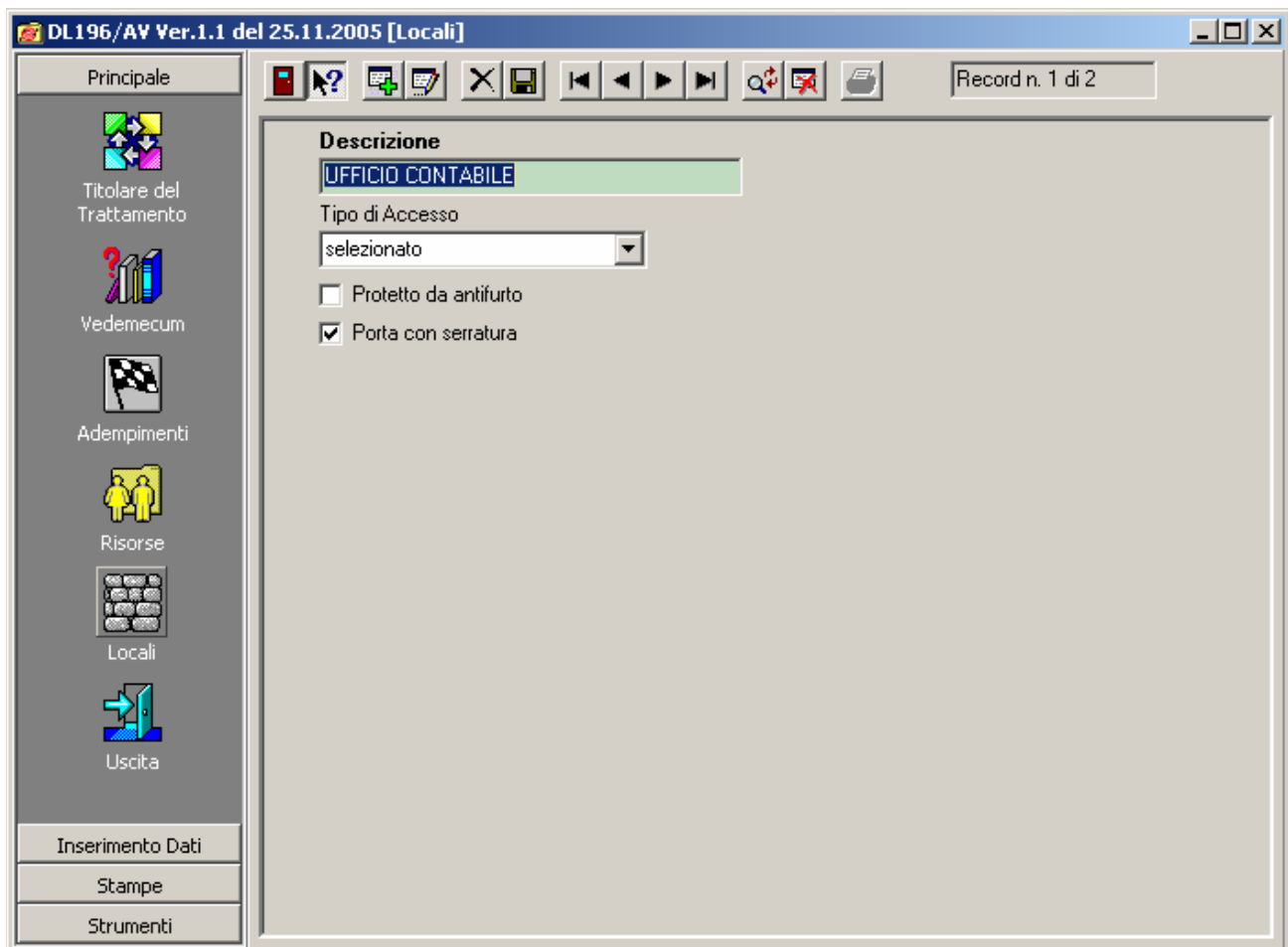
Una precisazione importante è che in questo archivio vanno riportati anche i soggetti esterni all'azienda a viene dato un incarico. I soggetti che probabilmente saranno spesso presenti sono gli studi professionali di consulenza tributaria, legale e del lavoro, a cui in questi casi verrà affidato il trattamento dati di terzi (per esempio nostri clienti, fornitori e dipendenti).

La legge dispone, giustamente, che questi trattamenti vadano gestiti con opportuni vincoli temporali e di riservatezza.

Il documento di nomina ad incaricato del trattamento stampato dal programma è leggermente diverso se la risorsa indicata è un professionista o una società terza, sottintendendo in questo caso che il trattamento avviene all'esterno, mentre in tutti gli altri casi il trattamento viene considerato svolto nei locali dell'azienda.

## 2.3 / LOCALI

Occorre ora definire i locali in cui viene effettuato il trattamento dei dati. E' bene ricordare che il termine "trattamento" è inteso in senso molto lato ed include esplicitamente anche la semplice consultazione.



Attenzione a definire con precisione il tipo di accesso, riepilogato dall'help contestuale che si attiva entrando nel campo "Tipo di Accesso". La legge prevede tre casi

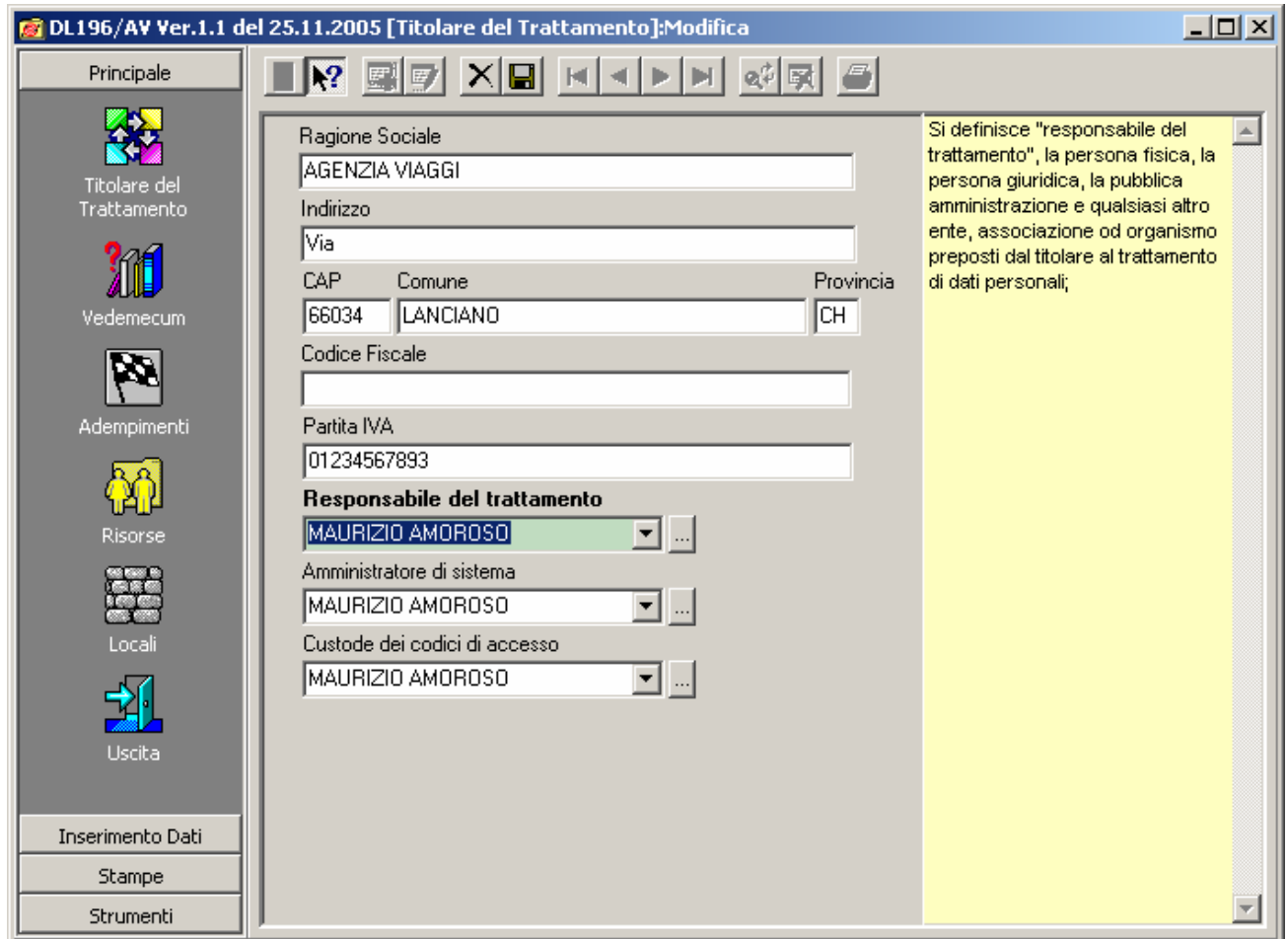
:

- Accesso Libero: Chiunque può entrare.
- Accesso Selezionato: Possono accedere solo i soggetti autorizzati (magari perché hanno le chiavi).
- Accesso Controllato: Gli accessi sono registrati in un apposito registro.

Le eventuali forme di protezione sono importanti nel caso di trattamento di dati sensibili o giudiziari.

## 2.4 IL RESPONSABILE

La legge individua tra le altre, la figura del responsabile del trattamento,



A questo punto, avendo inserito le risorse è possibile selezionare dalla lista la persona designata. La designazione di un responsabile è facoltativa, e nel caso non sia designato la sua figura coincide con il titolare del trattamento. In realtà potrebbero esserci più responsabili con competenze separate. Il responsabile rappresenta il titolare nei confronti degli incaricati, si attiene alle istruzioni indicate nella lettera di incarico e la sua nomina non dispensa il titolare dal vigilare sulla “puntuale osservanza” delle disposizioni impartite. In altre parole il responsabile non può essere visto come un capro espiatorio che sollevi il titolare dalle sue responsabilità. In particolare il responsabile deve essere scelto per le sue caratteristiche di “esperienza, capacità ed affidabilità che forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza” per cui è da escludere una sua funzione da “prestanome” essendo il titolare responsabile anche della sua scelta.

Il programma prevede un responsabile unico, inteso come elemento di riferimento dell’intera struttura, ed eventuali responsabilità diversificate possono essere definite nella tabella “Responsabilità” esposta in seguito.

Le altre due figure di riferimento (facoltative) da indicare sono:

- 1) Il responsabile di sistema, cioè colui che “sovrintende alle risorse software ed hardware degli elaboratori che gestiscono i dati”.

E' colui che deve comunque assicurarsi che il sistema informatico sia funzionale e protetto ed i software siano aggiornati. La sua nomina non è più obbligatoria, ma le sue responsabilità rimangono, quindi sarebbe opportuno nominarlo specificatamente.

- 2) il Custode dei codici di accesso, colui che “fisicamente assegna le password iniziali ai diversi incaricati e riceve ed archivia le password scelte dagli incaricati ed aggiornate periodicamente”

La dottrina prevede una procedura abbastanza contorta per la gestione delle password, in cui il custode, che può anche essere l'amministratore di sistema o il responsabile, assegna una password valida solo per il primo accesso, che viene consegnata all'utente in busta chiusa. Quando l'utente accede al sistema la modifica e dovrebbe restituire una copia al responsabile, sempre in busta chiusa. Lo scopo di questo turbinare di corrispondenza, è di ad avere la segretezza assoluta della password anche nei confronti dell'incaricato alla custodia delle password, ma allo stesso tempo la sua accessibilità in caso di necessità.

La password dovrebbe essere lunga almeno otto caratteri, essere modificata almeno ogni sei mesi, e non essere facilmente riconducibile all'utente a cui è associata, all'ente a cui appartiene o all'azienda. Se l'utente tratta dati sensibili la password andrebbe modificata ogni tre mesi.

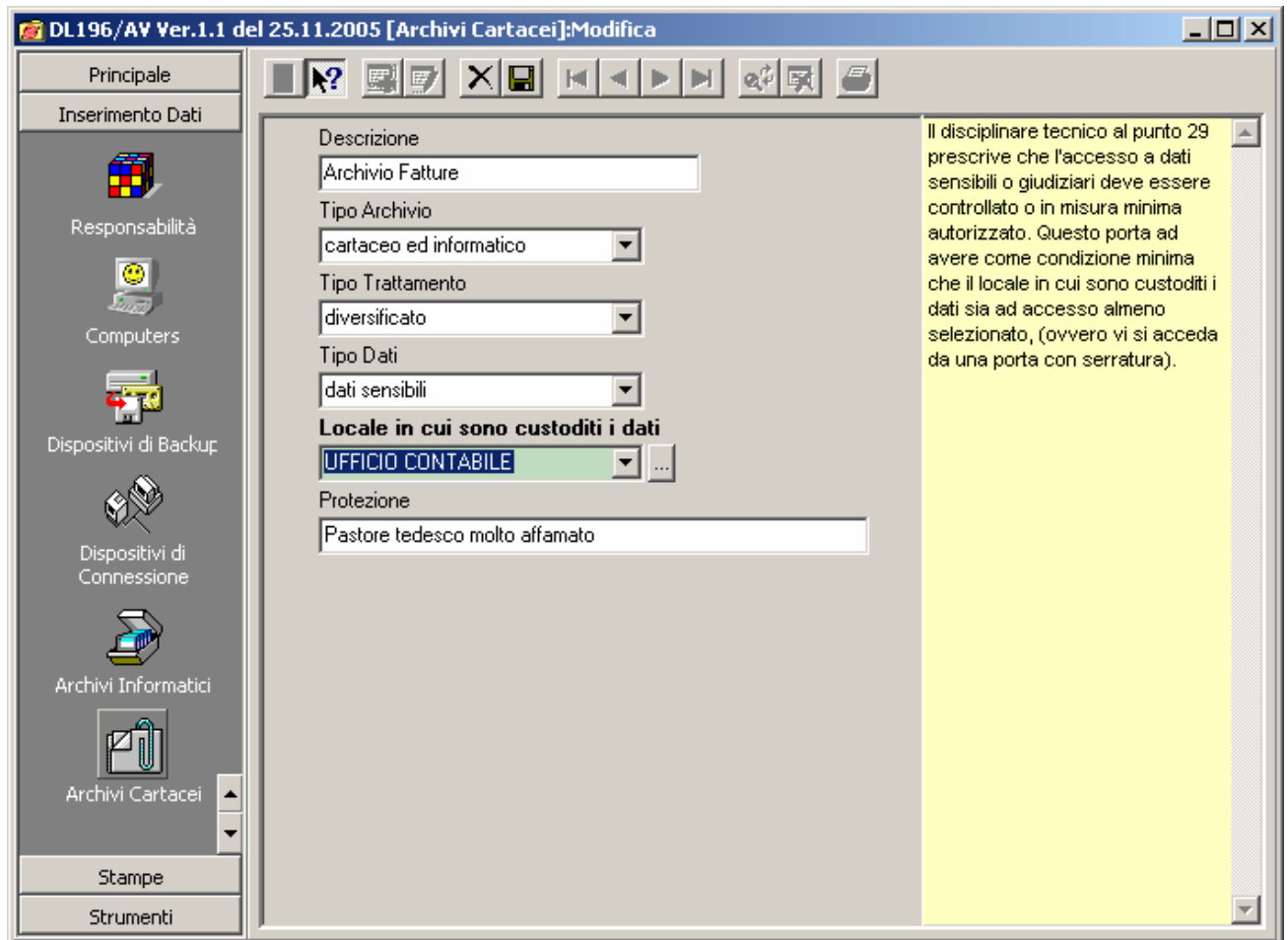
La legge non specifica se queste password sono da intendersi relative al sistema che gestisce i dati oggetto di trattamento, del sistema operativo o della macchina in se, ma sarebbe logico presumere che se il software applicativo non le supporta dovrebbe l'identificazione dell'utente dovrebbe essere almeno delegata al sistema operativo, e se questo non è possibile, andrebbe almeno impostata una password di accesso alla macchina.

In realtà la legge e successive circolari non ammetterebbero il trattamento elettronico di dati sensibili attraverso l'uso di attrezzature non idonee se non in via estremamente temporanea, per cui i sistemi andrebbero rapidamente adeguati. Al riguardo si fa presente che sistemi con sistemi operativi Windows 95, Windows 98 e Windows Millennium non garantiscono **alcuna** protezione da accessi non autorizzati poiché l'eventuale adozione di username e password riguarda solo il profilo di configurazione dell'utente e non l'accesso al computer. Windows 2000, Windows NT e XP **possono essere** configurati in modo da impedire l'accesso al computer se non si inseriscono correttamente username e password, tuttavia per accedere ai dati spesso è possibile rimuovere il disco fisso collegandolo come disco supplementare di una macchina a cui si ha accesso.

## 2.5 GLI ARCHIVI CARTACEI

Il trattamento dati più elementare e quasi certamente presente in azienda riguarda gli archivi cartacei. Occorre censire le tipologie di dati trattate su supporto cartaceo in azienda ed inserirle nell'apposito archivio.

Per inserire i dati degli archivi cartacei, selezionare il pannello “Inserimento Dati” e quindi il pulsante “Archivi Cartacei”.



Gli aspetti determinanti ai fini della sicurezza sono:

- 1) Il tipo di dati trattati:
  - a. Dati comuni, non riconducibili ad un particolare individuo o azienda
  - b. Dati personali
  - c. **Dati sensibili, e/o giudiziari.** In questo caso i dati debbono essere conservati in un locale con accesso almeno selezionato, ovvero consentito solo al personale specificatamente identificato ed autorizzato, (vedi figura).
- 2) Il tipo di trattamento, ovvero l'accesso previsto per gli incaricati, che può essere
  - a. Comune, in cui non ci sono differenze tra gli incaricati
  - b. Diversificato, in cui utenti diversi hanno diritti diversi. In questo caso sono fondamentali le cosiddette credenziali di identificazione degli utenti

## 2.6 I COMPUTERS

Il trattamento informatizzato prevede l'uso di computer, per cui prima di censire le tipologie di dati trattate informaticamente è opportuno censire gli elaboratori che accedono o su cui sono memorizzati i dati.

La schermata per l'introduzione dei dati sui computer è una delle più complesse presenti nel programma e si presenta come in figura:

DL196/AV Ver.1.1 del 25.11.2005 [Computers]

Principale

Inserimento Dati

Responsabilità

Computers

Dispositivi di Backup

Dispositivi di Connessione

Archivi Informatici

Archivi Cartacei

Incaricati del trattamento

Stampe

Strumenti

**Descrizione**

PC AGENZIA

Locale  
AGENZIA

Tipo Computer  
client

Sistema Operativo  
windows NT/2000/XP

Tipo Autorizzazione (Credenziali)  
username e password

Matricola

Con Floppy o altri supporti rimovibili  Protetto da Antivirus  
 Protetto da gruppo di Continuità  Protetto da Firewall

Connessione a reti esterne  
router su rete telefonica

Tipo di dati accessibili da questo computer  
dati comuni

Indirizzo IP      Tempo di ripristino  
                      60

Altro

I campi su cui può essere necessaria una spiegazione più approfondita sono i seguenti:

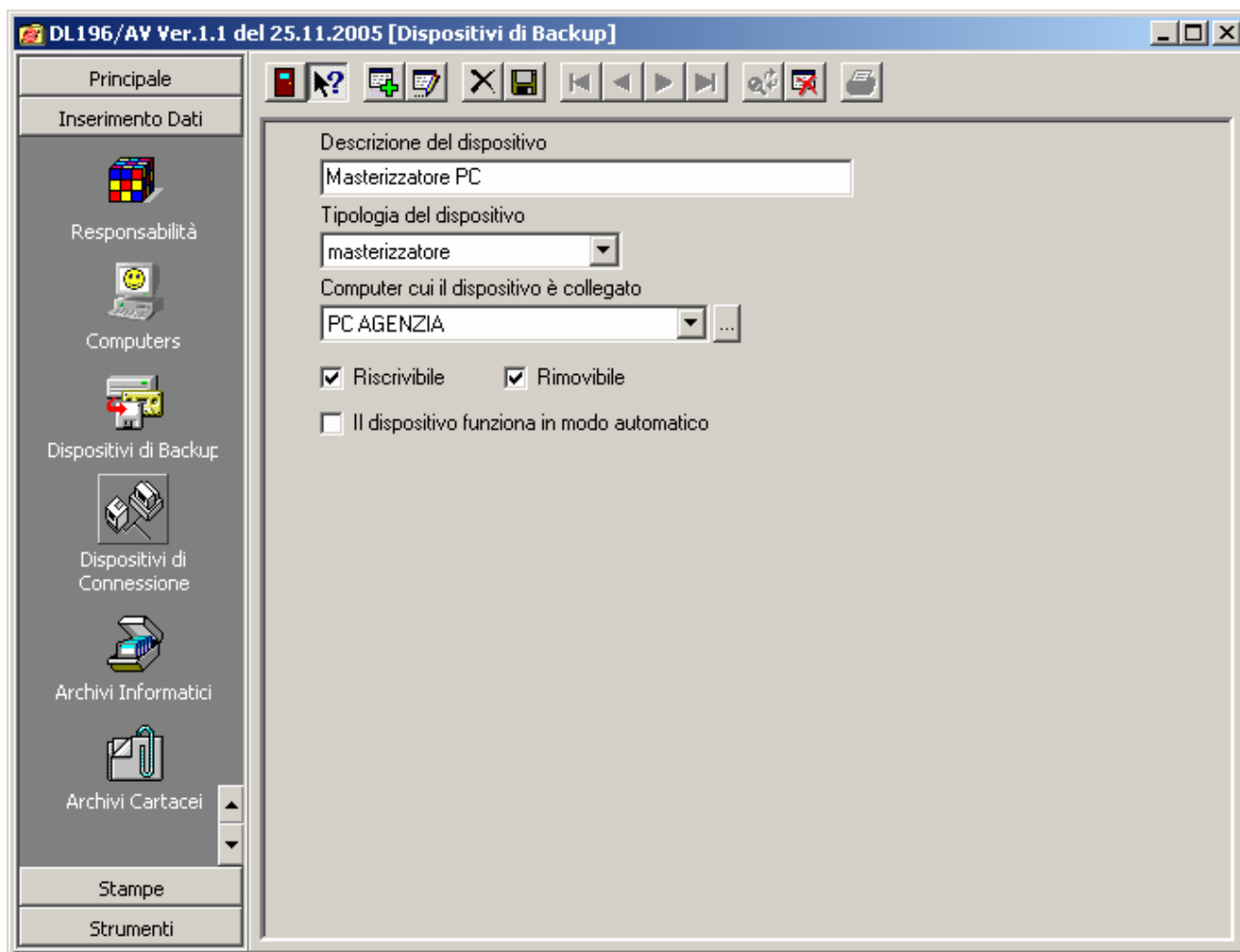
- 1) Tipo Computer: può essere
  - a. Client: Un computer che tratta dati memorizzati su un server
  - b. Computer con archivi condivisi: Un computer che tratta dati memorizzati su se stesso e accessibili da altri computer.

- c. Computer isolato: Un computer che tratta dati memorizzati su se stesso non accessibili da altri computer.
  - d. Portatile: Computer portatile.
  - e. Server: Computer utilizzato per il deposito e la condivisione di dati con altri computer, piuttosto che per il trattamento
- 2) Sistema operativo: Non tutti, (in verità pochi), i sistemi operativi consentono di gestire in modo efficace l'accesso diversificato in funzione dell'identità dell'utilizzatore. Per questo motivo un computer con sistema operativo Windows 95/98/Millennium non dovrebbe essere usato per accedere e meno ancora per conservare dati sensibili, se non vengono prese delle contromisure supplementari.
  - 3) Tipo di Autorizzazione: L'autenticazione informatica è l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utilizzatore. Le credenziali di autenticazione, sono i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica. Un computer che tratta o accede a dati sensibili non può prevedere un livello di autenticazione pari a "nessuno" se non sono poste in essere delle contromisure supplementari
  - 4) Con floppy o altri supporti rimovibili: Questi supporti possono essere utilizzati per asportare dati sensibili. Dove ci siano stringenti esigenze di sicurezza andrebbe considerata l'opportunità di disattivarli.
  - 5) Protetto da gruppo di continuità: La legge prescrive di prendere tutte le misure necessarie per salvaguardare l'integrità dei dati. Se il computer è un server o contiene o condivide degli archivi, sarebbe bene che ci fosse.
  - 6) Antivirus, Firewall, e Connessione a reti esterne: Per gli stessi motivi di cui sopra un software antivirus è una prescrizione praticamente obbligatoria mentre un firewall lo è se il computer è connesso ad internet attraverso un modem personale. Le ultime versioni del sistema operativo Windows XP (particolarmente il famigerato Service Pack 2), ne sono dotati all'origine.  
Computer con sistema operativo windows di versioni precedenti a quest'ultima possono essere facile preda di malintenzionati se si è connessi ad internet attraverso un modem locale. Questo è molto più difficile, ma non impossibile in tutti gli altri casi, tranne quello ovvio di computer non connesso ad Internet,
  - 7) Indirizzo IP: Questa caratteristica, è significativa solo in presenza di una rete locale, e si trova nel pannello di controllo, sull'oggetto Connessioni di rete, alla voce Rete Locale/Protocollo Internet (TCP/IP). Non ha alcuna importanza nell'ambito della legge sulla privacy ma in caso di emergenza può essere necessario conoscerle per un corretto ripristino della rete locale. Questo dato, se presente, viene riportato nel DPS per comodità dell'amministratore di sistema.

## 2.7 DISPOSITIVI DI BACKUP

La legge prescrive che il titolare è responsabile della integrità dei dati e deve prendere tutte le misure possibili per garantirla. La più ovvia è la creazione di copie di sicurezza, o di Backup.

Se sono trattati dati con tecnologia informatica questa voce non dovrebbe mancare.

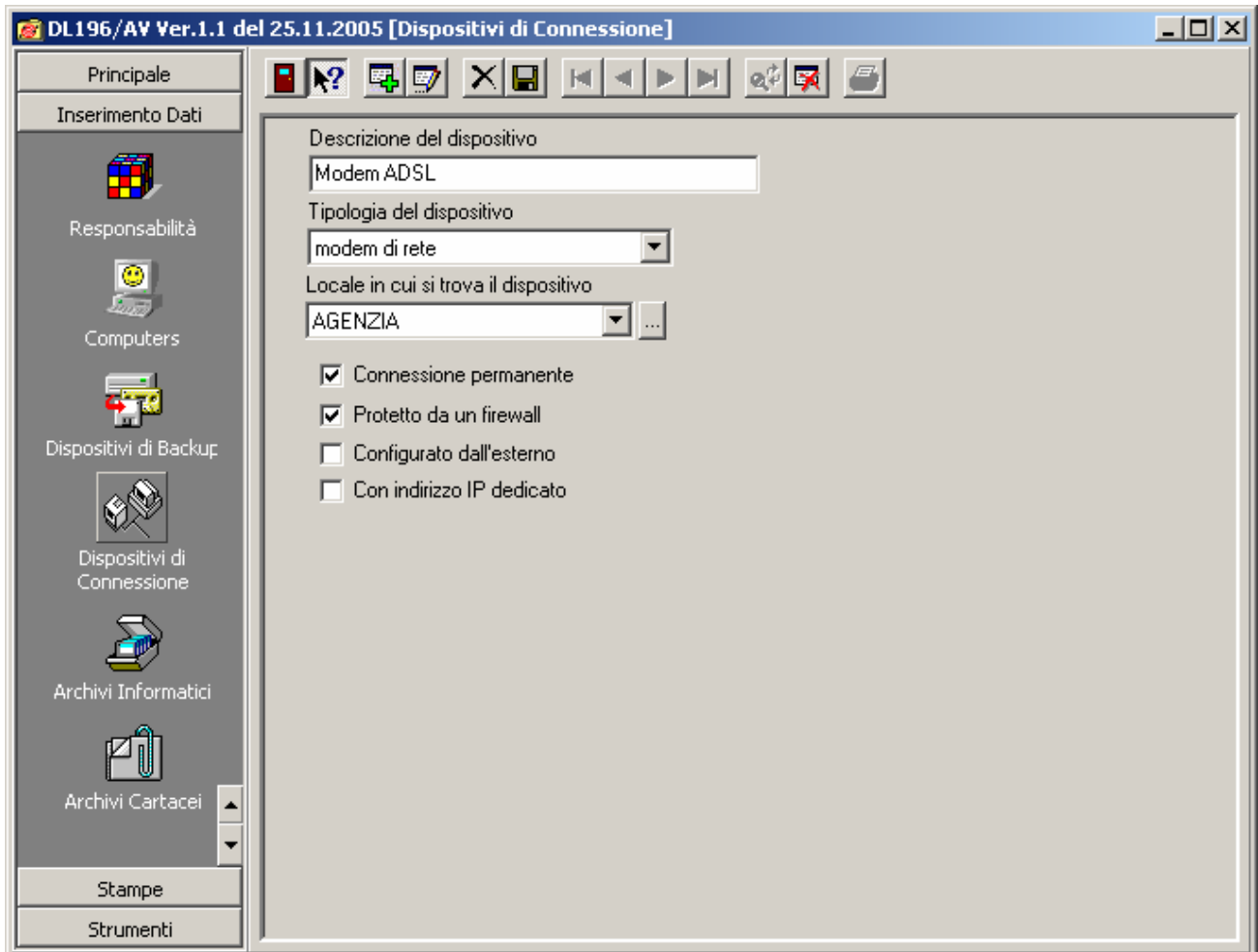


La legge prescrive che le copie di sicurezza vengano effettuate con periodicità almeno settimanale, lasciando libera la scelta delle modalità.

La soluzione più semplice ma meno affidabile è di usare un altro computer come dispositivo di backup, quella probabilmente più diffusa è quella di usare un masterizzatore per eseguire la copia su di un Compact Disk.. Il sistema ideale è una combinazione ridondante di più metodi che generino comunque una copia su un supporto rimovibile conservato in un luogo diverso da quello in cui si trovano i dati.

## 2.8 DISPOSITIVI DI CONNESSIONE

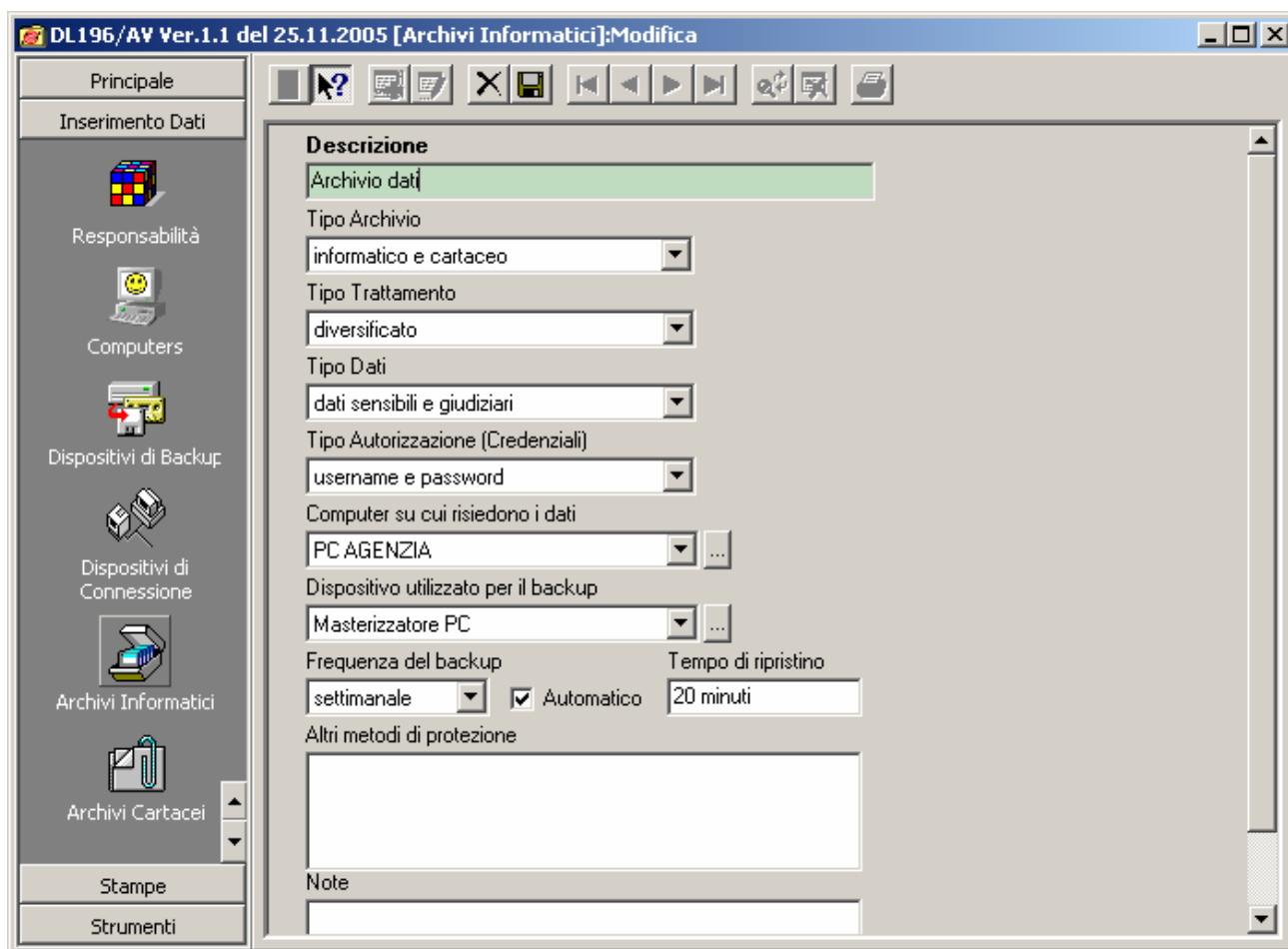
Occorre indicare nel DPS i dispositivi utilizzati per la connessione a reti esterne, tipicamente Internet.



## 2.9 GLI ARCHIVI INFORMATICI

Occorre a questo punto censire gli archivi informatici presenti in azienda.

Il programma consente specificare delle combinazioni che sono in violazione ai requisiti minimi di sicurezza, ma ciò non dipende dalla mancanza di controlli sull'input digitato. Va tenuto conto che andrebbe descritta la realtà e non una situazione di compiacente ma ipocrita aderenza alle prescrizioni di legge. Possono essere stati posti in essere altri metodi di protezione e espone nelle note delle motivazioni per cui la configurazione descritta è almeno per il momento adottata.



Dati sensibili non dovrebbero risiedere su macchine con sistema operativo non sicuro o senza l'adozione di credenziali di autorizzazione, così come un trattamento diversificato ha poco senso senza l'identificazione dell'utente.

Nella sezione Strumenti c'è il pulsante "Verifica Dati Immessi" che produce una stampa che evidenzia le difformità dalle prescrizioni di legge indicando dove e come intervenire (realmente) per soddisfare i requisiti delle misure minime di sicurezza.