Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

Allegato A

Modalità di gestione del giornale degli affari secondo modalità informatiche

1 Contenuti

Il registro degli affari (di qui in avanti il *Registro*), deve indicare:
1) nome, cognome e domicilio del committente ed estremi del documento di identificazione;
2) la data e natura della commissione (attività di gestione, di recupero per conto terzi, servizio connesso o strumentale);
3) il premio pattuito, esatto o dovuto; modalità di pagamento da parte del mandante;
4) l'esito dell'operazione;
5) nome cognome e domicilio del debitore (ovvero del soggetto che effettua il pagamento per suo conto) ed estremi del documento di identificazione solo in ipotesi di successo dell'attività di recupero e pagamento tramite conti correnti della soc. di tutela del credito.

2 Formati

Per l'inserimento informatico delle annotazioni devono essere adottati formati che, al minimo, possiedano requisiti di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura. In via preferenziale devono adottarsi i formati XML, PDF-A, HTML, TXT, TIFF, ecc.

3 Sistema di gestione informatica del protocollo e dei documenti

Il sistema operativo dell'elaboratore, su cui è realizzato il sistema di gestione informatica del Registro deve essere conforme alle specifiche previste dalla normativa vigente e deve assicurare:

a) l'univoca identificazione ed autenticazione degli utenti che procedono all'inserimento dei dati;
b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso.
Le annotazioni devono essere protette da modifiche non autorizzate.

Il sistema inoltre:

Ministero dell'Interno
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

1) deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;

2) deve assicurare il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

La conformità del sistema operativo alle specifiche di cui sopra sono attestate dall'amministratore di sistema con idonea documentazione.

4 Registro informatico

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del Registro deve essere riversato:
- al termine della giornata lavorativa, su supporti riscrivibili e conservato a cura dell'amministratore di sistema;
- ogni trenta giorni su supporto non riscrivibile;
- trimestralmente su supporto non riscrivibile e conservato a cura dell'amministratore di sistema e consegnandone copia alla Questura.

Alla chiusura delle registrazioni, il contenuto annuale del Registro deve essere riversato, in triplice copia, su un supporto informatico non riscrivibile.

5 Sicurezza fisica dei documenti

Il Titolare del trattamento o, per suo conto, il Responsabile o l'Amministratore di sistema appositamente nominati, deve garantire la puntuale esecuzione delle operazioni di backup dei dati e dei documenti registrati, su supporti informatici non riscrivibili.

Le copie di backup dei dati e dei documenti prodotte in almeno tre copie sono conservate a cura dei predetti soggetti in un luogo diverso dalla sede.

6 Gestione della riservatezza

1) ad ogni annotazione, all'atto della registrazione nel sistema, deve essere associata una Access Control List (ACL) che consenta di stabilire quali utenti o gruppi di utenti abbiano accesso ad esso. Per default il sistema deve seguire la logica dell'organizzazione, in modo che ciascun utente possa accedere solamente ai documenti che siano stati assegnati alla sua struttura di appartenenza, o agli uffici ad esso subordinati;

Ministero dell'Interno
DIPARTIMENTO DELLA PUBBLICA SICUREZZA

2) il titolare del trattamento ha l'obbligo di predisporre un mansionario contenente le regole per l'accesso al Registro da parte degli incaricati sulla base della normativa vigente in materia di privacy.
3) il controllo degli accessi ai dati di protocollo e alla base documentale da parte del personale dell'amministrazione deve essere assicurato mediante un sistema di credenziali di autenticazione ed autorizzazione, secondo quanto previsto dall'All. B) al D.Lgs. 196/2003;
4) il servizio informatico deve assicurare, come previsto dal Documento programmatico sulla sicurezza, la variazione sistematica delle password assegnate agli utenti per l'accesso alle funzioni del sistema di protocollo informatico.

7 Supporti di memorizzazione

Per l'archiviazione ottica dei documenti devono essere utilizzati supporti di memorizzazione digitale che consentano la registrazione mediante la tecnologia laser (WORM, CD-R, DVD-R).

8 Tenuta del Registro

Il Responsabile del procedimento di conservazione digitale (Conservatore) deve:

a) adottare le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza;

b) ogni trenta giorni rendere statico il dato dinamico contenuto nel registro mediante una copia di back up non modificabile ovvero mediante la duplicazione del dati contenuti nel registro, su un supporto informatico non alterabile e conservarlo per 10 anni;

c) verificare periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti;

d) deve consegnare copia alla Questura del registro su supporto non modificabile ogni tre mesi.