D.M. 27 aprile 2009

Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia.

Pubblicato nella Gazz. Uff. 11 maggio 2009, n. 107.

IL MINISTRO DELLA GIUSTIZIA

Vista la *legge 2 dicembre 1991, n. 399*, recante: «Delegificazione delle norme concernenti i registri che devono essere tenuti presso gli uffici giudiziari e l'amministrazione penitenziaria»;

Visto l'*art. 206 del decreto legislativo 28 luglio 1989, n. 271* recante le Norme di attuazione, di coordinamento e transitorie del Codice di Procedura Penale;

Visto il *decreto legislativo 12 febbraio 1993, n. 39*, recante: «Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, ai sensi dell'*art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421*»;

Visto il *decreto del Presidente della Repubblica 28 ottobre 1994, n. 748*, recante il regolamento sulle modalità applicative del *decreto legislativo 12 febbraio 1993, n. 39*, in relazione all'amministrazione della giustizia;

Visto il *decreto legislativo 30 giugno 2003, n. 196*, recante: «Codice in materia di protezione dei dati personali»;

Visto il *decreto legislativo 7 marzo 2005, n. 82*, recante: «Codice dell'Amministrazione digitale»;

Visto il *decreto 27 marzo 2000, n. 264*, del Ministro della giustizia, pubblicato nella Gazzetta Ufficiale del 26 settembre 2000, n. 225, recante il regolamento sulla tenuta dei registri presso gli uffici giudiziari;

Visto l'*art. 1, comma 1, lettera f), del citato decreto n. 264 del 2000*, che prevede l'emanazione di regole procedurali;

Visto il *decreto ministeriale 24 maggio 2001* concernente: «Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia», pubblicato nella Gazzetta Ufficiale del 5 giugno 2001, n. 128;

Visto il parere reso dal Centro per l'informatica nella pubblica amministrazione in data 29 maggio 2008;

Consultato il Garante per la protezione dei dati personali;

Decreta:

Art. 1.

1. Il presente decreto fissa, in sostituzione del *decreto ministeriale 24 maggio 2001*, le regole procedurali per la gestione del sistema informatico del Ministero della giustizia e per la tenuta informatizzata dei registri informatizzati tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari, ovvero ai registri previsti da codici, da leggi speciali o da regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dall'amministrazione della giustizia, come previsti dall'*art. 1 del decreto ministeriale 27 marzo 2000, n. 264*.

2. Per le modalità di tenuta informatizzata dei registri e per la sottoscrizione con firma digitale dei documenti informatici si tiene conto anche delle regole tecniche emanate ai sensi del *decreto legislativo 7 marzo 2005, n. 82*«Codice dell'Amministrazione digitale».

3. Le regole procedurali di cui al comma 1 sono riportate nell'allegato al presente decreto.

Allegato ex *art. 1*
Regole procedurali per la tenuta dei registri informatizzati degli uffici

Art. 1 *Definizioni*

1. Ai fini del presente decreto si intende per:

a) Sistema informativo: l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione (sia in formato cartaceo sia elettronico) che, nel loro complesso, consentono qualunque operazione o complesso di operazioni, concernenti il trattamento dei dati e delle informazioni anche personali relativi alla tenuta dei registri connessi all'espletamento delle attribuzioni e dei servizi svolti dalla Amministrazione della giustizia.

b) Sistema informatico: la parte del sistema informativo che gestisce informazioni con tecnologia informatica e, per estensione, le sale server ovvero i locali attrezzati che ospitano i sistemi server.

c) Risorse informatiche: hardware, software, apparati di rete e cablaggi, sale server.

d) Servizi informatici: le risorse informatiche e i servizi per loro tramite forniti, sia di natura applicativa sia sistemistica.

e) Amministrazione: il Ministero della giustizia.

f) D.G.S.I.A.: la Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della giustizia.

g) Responsabile S.I.A.: il responsabile per i sistemi informativi automatizzati ai sensi dell'*articolo 10 del decreto legislativo 12 febbraio 1993,*

n. 39, quale direttore generale della D.G.S.I.A.

h) C.I.S.I.A.: Coordinamento Interdistrettuale per i Sistemi Informativi Automatizzati, articolazione territoriale della D.G.S.I.A., come prevista dal *D.M. 18 dicembre 2001* e successive modifiche.

i) Dirigente informatico: il dirigente amministrativo in possesso dei requisiti di cui all'*art. 11 del decreto legislativo 12 febbraio 1993, n. 39* e preposto alla direzione di un C.I.S.I.A. o i un ufficio della D.G.S.I.A.

j) ADSI: l'amministratore dei servizi informatici.

k) Fornitore qualificato: il fornitore ricompreso negli elenchi di fornitori a livello nazionale e regionale di cui all'*art. 82 del decreto legislativo 7 marzo 2005, n. 82* e successive modificazioni.

l) Struttura per la sicurezza del distretto: organizzazione per la sicurezza informatica degli uffici giudiziari del distretto.

Art. 2 *Requisiti del sistema informatico*

1. Il sistema informatico soddisfa i seguenti requisiti:

a) disponibilità: i dati sono formati, raccolti, conservati, resi disponibili e accessibili in modo da assicurarne l'uso interno e la fruizione, anche in caso di eventi interruttivi del funzionamento dei sistemi, compatibilmente con i livelli di servizio prestabiliti;

b) integrità: i dati sono trattati in modo da assicurarne precisione, completezza e inalterabilità;

c) autenticità: la provenienza dei dati è garantita e asseverata;

d) controllo degli accessi fisici e logici: le informazioni possono essere fruite solo ed esclusivamente dalle persone autorizzate a compiere tale operazione.

Art. 3 *Organizzazione del sistema informatico*

1. Il sistema informatico del Ministero della giustizia è articolato a livello nazionale, interdistrettuale, distrettuale e locale.

2. Il livello nazionale è costituito dalle componenti relative agli uffici dell'Amministrazione centrale, della Corte di Cassazione, della Procura Generale presso la Corte di Cassazione, del Tribunale Superiore delle Acque Pubbliche e della Direzione Nazionale antimafia e da quelle relative all'erogazione di servizi comuni o centralizzati.

3. Il livello interdistrettuale è costituito dalle componenti relative agli uffici di più distretti di Corte di Appello e da quelle relative all'erogazione di servizi comuni agli ambiti di uffici di più distretti.

4. Il livello distrettuale è costituito dalle componenti relative agli uffici della

sede di distretto di Corte di Appello e da quelle relative all'erogazione di servizi comuni agli ambiti distrettuale e locale.

5. Il livello locale è costituito dalle componenti relative agli uffici periferici del distretto di Corte di Appello.

6. Le strutture elaborative serventi sono allocate in corrispondenza delle componenti di cui ai commi precedenti.

7. Il Responsabile S.I.A. emana ed aggiorna periodicamente, con proprio decreto, le linee guida per la organizzazione e gestione del sistema informatico. Le linee guida sono rese note con gli opportuni strumenti di comunicazione ed in ogni caso sul portale internet dell'Amministrazione.

Art. 4 *Amministratore dei servizi informatici*

1. L'amministratore dei servizi informatici (ADSI) assicura la conduzione operativa di specifiche componenti del sistema informatico, effettuando, anche mediante accesso remoto, tutte le operazioni necessarie a garantire i requisiti di cui all'*art. 2*.

2. Un coordinatore degli ADSI viene nominato qualora vi sia la necessità che più amministratori operino su componenti identiche o affini del sistema informatico.

3. E' in ogni caso prevista la nomina di un coordinatore degli ADSI per ciascuna delle sale server nazionali, interdistrettuali e distrettuali.

4. Il Responsabile S.I.A., su proposta del dirigente informatico competente per territorio o per settore, designa i soggetti di cui ai commi 1, 2 e 3, individuandoli fra gli esperti informatici dell'Amministrazione ovvero, se non sono disponibili tali risorse, ricorrendo a personale esterno qualificato.

5. L'amministratore dei servizi informatici, se nominato responsabile del trattamento da parte dei titolari delle banche dati, pone in essere le iniziative necessarie per il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri, anche alla luce delle direttive concordemente emanate dai titolari delle banche dati.

6. In ogni caso, l'amministratore dei servizi informatici garantisce che il capo dell'ufficio giudiziario, o un suo delegato, possa accedere alla infrastruttura logistica condivisa per verificare il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri.

Art. 5 *Identificazione delle componenti del sistema informatico*

1. La D.G.S.I.A. produce e mantiene aggiornato un dettagliato inventario di tutti gli elementi facenti parte del sistema informatico.

2. La D.G.S.I.A. definisce la struttura dell'inventario ed i criteri di accesso e conservazione delle informazioni in esso contenute.

3. L'amministratore dei servizi informatici predispone un dettagliato inventario delle componenti del sistema informatico di sua competenza secondo la struttura di cui al comma 2 e lo mantiene aggiornato ogni qualvolta si verifica una variazione.

4. L'inventario di cui al comma 1 è reso disponibile a tutti gli uffici interessati.

Art. 6 *Piano di distribuzione delle risorse informatiche*

1. L'amministratore dei servizi informatici redige il piano delle risorse informatiche da dedicare all'erogazione dei servizi messi a disposizione degli uffici e lo trasmette al dirigente informatico competente ed agli uffici interessati.

2. La D.G.S.I.A. pianifica la destinazione delle risorse che compongono il sistema informatico in coerenza con i servizi che devono essere erogati, tenendo conto dei piani di cui al comma 1.

Art. 7 *Gestione della sicurezza del sistema informativo*

1. Il Responsabile S.I.A. predispone il documento programmatico della sicurezza di cui all'*art. 34 del decreto legislativo 30 giugno 2003, n. 196*, relativamente alle componenti del sistema informatico dell'Amministrazione, che sono centralmente gestite e controllate.

2. Gli uffici, con la collaborazione tecnica del CISIA competente, predispongono il documento programmatico della sicurezza di cui all'*art. 34 del decreto legislativo 30 giugno 2003, n. 196*, relativamente al sistema informativo di propria competenza e lo rendono disponibile al Responsabile S.I.A.

3. Per le infrastrutture logistiche comuni il piano è predisposto in modo condiviso dagli uffici.

4. La vigilanza sulla applicazione dei documenti di cui ai precedenti commi 1 e 2, è esercitata dal Responsabile S.I.A., o da suoi delegati, che segnala

eventuali difformità comportamentali ai capi degli uffici ed adotta, in caso di urgenza, le misure e i provvedimenti necessari ad assicurare il corretto funzionamento del sistema informatico.

Art. 8 *Politica di gestione degli accessi*

1. Ogni utente, preliminarmente all'accesso alle risorse del sistema informatico, è identificato tramite procedure di autenticazione, definita e gestita dal Responsabile S.I.A.

2. Il Responsabile S.I.A. individua ed aggiorna periodicamente, con proprio decreto, la procedura di autenticazione. L'autenticazione prevede, come misura minima per l'identificazione, la conoscenza di una coppia di informazioni (username e password), secondo quanto previsto dal disciplinare tecnico di cui all'Allegato B del Codice in materia di protezione dei dati personali.

3. Ogni utente ottiene, tramite la procedura di autorizzazione, uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo di autorizzazione, rispetto alle risorse del sistema informatico.

4. A ciascun insieme omogeneo di utenti è associato un solo profilo; a ciascun utente può essere assegnato uno o più profili.

5. Ogni profilo è definito in modo tale da assegnare a ciascun utente solo ed esclusivamente i privilegi strettamente necessari per l'espletamento delle attività di propria competenza.

6. La struttura per la sicurezza del distretto individua i referenti degli uffici per l'assegnazione agli utenti dei profili relativi al trattamento dei dati.

7. Il Responsabile S.I.A., o suoi delegati, assegna agli amministratori dei servizi informatici uno o più profili volti alla conduzione, anche remota, dei sistemi e delle postazioni di lavoro e ne dà comunicazione agli uffici interessati.

Art. 9 *Salvataggio e conservazione dei dati*

1. Il Responsabile S.I.A. definisce, con proprio decreto, le politiche e le procedure per il salvataggio (backup) e per il recupero (recovery) dei dati.

2. Nell'ambito delle misure di cui al comma 1, la frequenza del salvataggio dei dati avviene con cadenza almeno giornaliera.

3. Le procedure di backup consentono di conservare i dati secondo le regole tecniche emanate ai sensi degli *articoli 22* e *71 del decreto legislativo 7 marzo*

2005, n. 82.

4. Le procedure di backup consentono di effettuare, con frequenza almeno triennale, una copia storica dei dati, che dovrà essere conservata secondo le modalità di cui al comma 3. Eseguita tale operazione, dal registro in uso possono essere eliminati i dati relativi agli affari esauriti da almeno due anni.

5. Il sistema di consultazione della copia storica dei dati ne garantisce la leggibilità nel tempo e l'autenticità, secondo le regole tecniche emanate ai sensi degli *articoli 22* e *71 del decreto legislativo 7 marzo 2005, n. 82*.

Art. 10 *Monitoraggio del sistema*

1. Le attività relative all'utilizzo e alla gestione del sistema informatico, anche da remoto, sono sottoposte ad un processo continuo di controllo e verifica della loro corretta e completa esecuzione. Il processo di controllo e verifica si attua anche attraverso l'utilizzo di appositi strumenti di controllo a livello di sistema, di database management system, di applicativo e di postazione di lavoro.

2. Il sistema informatico prevede, a garanzia della autenticità e della integrità dei dati e come misura minima di monitoraggio, la registrazione di tutti gli accessi, anche di carattere tecnico, ivi compresi quelli non riusciti o falliti, e di tutte le operazioni effettuate sui dati.

3. La D.G.S.I.A. si dota degli strumenti di monitoraggio di cui al comma 1, per consentire al personale tecnico di svolgere le opportune verifiche. La D.G.S.I.A. è responsabile delle attività di cui al comma 1 e vigila sullo svolgimento delle stesse, anche se affidate a personale esterno specificamente individuato.

4. Le registrazioni dei log delle attività di cui al comma 1, devono essere trascritte con cadenza almeno settimanale su supporti non riscrivibili da conservare unitamente ai backup.

5. La struttura per la sicurezza del distretto, i titolari ed i responsabili per il trattamento dei dati hanno facoltà di esaminare, nell'ambito delle rispettive competenze, le registrazioni di cui al comma 4.

Art. 11 *Infrastruttura logistica*

1. Il Responsabile S.I.A. predispone, con proprio decreto, le linee guida per l'allestimento dei locali adibiti a sale server.

2. Le linee guida di cui al comma 1, prevedono almeno le indicazioni relative alla localizzazione e predisposizione tecnologica delle sale server, alle procedure per l'accesso alle sale server ed alle procedure per la conservazione

fisica dei supporti di backup.

3. Il Responsabile S.I.A., se non vi è disponibilità di locali di proprietà o messi a disposizione dell'Amministrazione giudiziaria, ha facoltà di utilizzare sale server di fornitori qualificati che rispondono alle linee guida di cui al comma 1.

4. Il dirigente informatico è responsabile della gestione delle sale server nel territorio o settore di sua competenza. Egli può delegare alcune di tali attività ad un ADSI.

5. Il dirigente informatico, o persona dallo stesso delegata, partecipa alle riunioni della Commissione di manutenzione di cui alla *legge 24 aprile 1941, n. 392*, nel territorio assegnato alla sua competenza.

Art. 12 *Software*

1. E' consentito installare ed utilizzare unicamente il software preventivamente approvato dal Responsabile S.I.A. secondo quanto previsto dall'*articolo 3, comma 2, del decreto ministeriale 27 marzo 2000, n. 264*.

2. L'elenco dei software nazionali con le relative funzionalità fornite è pubblicato sul sito dell'Amministrazione.

3. Non è consentito utilizzare o sperimentare software, in deroga a quanto previsto al comma 1, salvo specifica autorizzazione del Responsabile S.I.A.

4. Il software è installato esclusivamente a partire da supporti fisici originali, ovvero per i quali sia nota e sicura la provenienza.

5. Il software e la relativa documentazione, realizzati per conto della D.G.S.I.A., sono prodotti in maniera conforme alle regole tecniche dettate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

Art. 13 *Dati in formato elettronico*

1. L'accesso ai dati da parte degli utenti avviene esclusivamente per il tramite del software di cui all'*articolo 12*.

2. Tutte le operazioni di manutenzione effettuate sui dati sono soggette ad autorizzazione e registrazione secondo quanto previsto dall'*articolo 10*.

3. Il dirigente o responsabile dell'ufficio è responsabile della qualità dei dati e ne verifica periodicamente, anche attraverso il personale dell'ufficio all'uopo incaricato ed anche utilizzando strumenti automatici, correttezza ed

aggiornamento, assumendo le conseguenti iniziative.

4. Il dirigente o responsabile dell'ufficio può nominare uno o più delegati per le attività di controllo sui dati di propria competenza.

5. La delega di cui al comma precedente è attribuita al personale dell'ufficio o, nel caso previsto dall'*articolo 3*, di altro ufficio.

Art. 14 *Applicativi per la tenuta dei registri*

1. L'applicativo è accompagnato da apposita documentazione di utilizzo, costituita da un manuale di amministrazione ed un manuale di utilizzo, disponibile sia in forma cartacea che in forma elettronica.

2. Il Responsabile S.I.A. predispone, con proprio decreto, le linee guida per la redazione della documentazione di cui al comma precedente.

Art. 15 *Disposizioni per la salvaguardia dei dati*

1. Il Responsabile S.I.A. definisce, con proprio decreto, la politica della sicurezza dei sistemi informatici della giustizia.

2. Il Responsabile S.I.A. adotta, con il decreto di cui al comma 1, o con successivo provvedimento, le linee guida relative, fra l'altro, a:

a) modalità di gestione delle utenze;
b) modalità di comportamento delle utenze agli effetti della sicurezza informatica;
c) controllo fisico e logico degli accessi ai sistemi informatici;
d) politiche, modalità esecutive e strumenti per la salvaguardia dei dati (backup, disaster recovery, ecc.);
e) politiche e modalità esecutive per la conservazione e la riproduzione dei supporti fisici dei dati;
f) gestione dei sistemi di protezione dagli attacchi informatici (antivirus, antispam, firewall, IDS, IPS, ecc.);
g) modalità e strumenti di supporto per il controllo e il monitoraggio della sicurezza informatica;
h) procedure di verifica e controllo dei livelli di sicurezza informatica;
i) politiche per la formazione degli utenti in tema di sicurezza informatica.