ALLEGATO AL RENDICONTO GENERALE 2006

- DOCUMENTO PROGRAMMATICO SULLA SICUREZZA -

PAGINA BIANCA

ENPALS		*Emesso da: Direzione Sistemi Informativi e Telecomunicazioni - DSIT*

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi dell'articolo 34, comma 1, lettera g)
e Allegato B - Disciplinare Tecnico, Regola 19
del Decreto legislativo 30 Giugno 2003 n.196
"Codice in materia di protezione dei dati personali"

Aggiornato il 5 dicembre 2006

Sommario

1 Premessa metodologica

Il presente Documento Programmatico sulla Sicurezza è redatto dall'ENTE NAZIONALE DI PREVIDENZA E ASSISTENZA DEI LAVORATORI DELLO SPETTACOLO (di seguito semplicemente ENPALS), con sede in Roma in viale Regina Margherita, 206, a cura del Responsabile della Direzione Sistemi Informativi e Telecomunicazioni (nel seguito DSIT), con il concorso dei Responsabili del trattamento dei dati.

Il Documento è stato elaborato sulla base della disciplina in materia di tutela dei dati personali - D.lgs. 196/2004 - e delle disposizioni di Sicurezza dettate dal Disciplinare Tecnico di cui all'Allegato B della medesima Legge.

Per la redazione della presente versione, che costituisce l'aggiornamento della precedente (Delibere commissariali n. 759 del 23.6.2004 e n. 761 del 30.6.2004), del Documento Programmatico sulla Sicurezza (nel seguito DPS) è stata effettuata una ricognizione di tutti i trattamenti di dati personali svolti presso l'ENPALS o affidati a soggetti terzi.

A tal fine è stata adottata una metodologia di sviluppo del documento, meglio descritta nel seguito, che ha portato a rilevare i processi di lavoro negli uffici centrali e periferici al fine di individuare le basi dati di interesse ai fini della privacy e individuare i soggetti fisici e giuridici (sia interni sia esterni) che svolgono operazioni di trattamento dei dati e che sono abilitati a svolgerle.
La rilevazione dei processi di trattamento ha consentito, contestualmente, di individuare i sistemi, le infrastrutture tecnologiche sottese al trattamento e le aree di loro localizzazione.
L'analisi del ciclo di lavorazione dei dati ha riguardato sia i trattamenti svolti con strumenti elettronici, sia i trattamenti relativi ad atti e documenti cartacei.

A seguito delle attività di rilevazione effettuate, è stato accertato il risultato dell'analisi dei rischi per stabilirne l'efficacia e completezza rispetto alle minacce di distruzione e perdita dei dati (anche accidentale), di accessi non autorizzati, di trattamenti non consentiti o non conformi rispetto alle finalità della raccolta.
Il risultato degli accertamenti unitamente alle considerazioni emerse e di seguito descritta nell'apposito capitolo.

Per ogni trattamento sono state censite e valutate le misure di sicurezza poste in essere al fine di determinare la loro corrispondenza e adeguatezza, con quanto previsto dalla Legge 196/03 e correlato Disciplinare tecnico; sono state esaminate le deliberazioni in materia e le istruzioni normative interne che disciplinano la politica interna sulla *Data Privacy*, osservati gli ambienti e i locali di lavoro nei quali avvengono i trattamenti.

A fronte di quanto innanzi descritto, è stato redatto il presente documento programmatico sulla sicurezza.

Il documento è stato impostato in diversi capitoli, organizzati in maniera da rappresentare le disposizioni di cui alla regola 19 del Disciplinare tecnico della Legge.

1.1 Politica interna sulla riservatezza dei dati

Lo scopo del presente documento è quello di descrivere le modalità di trattamento delle informazioni effettuate presso l'ENPALS, sotto il profilo della sicurezza e riservatezza dei dati, al fine di attestarne la qualità, la puntualità e l'osservanza alle previsioni di legge.

La protezione dei dati conferiti (dai dipendenti, dai cittadini, dai fornitori, nonché di tutte le persone fisiche e giuridiche con cui quotidianamente l'ENPALS viene a contatto) è prioritaria e fondamentale per l'esecuzione delle attività istituzionali di questo Ente.

Per questo motivo l'ENPALS dedica la massima attenzione ed il massimo impegno, anche economico, alla tematica della sicurezza dei dati, adottando le misure tecnologiche organizzative e logistiche più adeguate a garantire una appropriata copertura dei rischi derivanti dalla perdita, sia dolosa sia accidentale, dell'integrità, riservatezza e disponibilità dei dati stessi.

L'ENPALS è altresì consapevole che la sicurezza non è un processo statico, ma dinamico, che deve essere sempre aggiornato alle mutate esigenze quali, ad esempio, il rilascio di nuovi servizi informatici, l'affacciarsi di nuovi rischi, la disponibilità di nuove tecnologie, etc.

1.2 Policy di sicurezza

Il documento è stato predisposto ad uso interno allo scopo di rendere pubbliche e applicabili le regole di sicurezza anche ai fini della conformità alle disposizioni di Legge.

Il documento in questione descrive le politiche di sicurezza dei sistemi informativi rappresentando l'insieme delle norme e regolamenti che indicano come le informazioni e le risorse tecnologiche sono gestite e protette nell'ambito del Sistema Informativo.

La valutazione del rischio è focalizzata ad evidenziare la gradualità delle aree di rischio del sistema informativo, al fine di individuare gli interventi di protezione.

Le funzioni di sicurezza sono indipendenti dalle tecnologie utilizzate e indicano i riferimenti generali per la protezione dei dati. Tale protezione è assicurata dal sistema su tutte le tecnologie in cui i dati vengono memorizzati, elaborati o trasportati. Le funzioni di sicurezza sono state divise in tre tipologie, ovvero hardware/software, organizzative e logistiche.

Le funzioni di sicurezza vengono realizzate da meccanismi di sicurezza che identificano l'algoritmo, l'apparato, il prodotto software o procedura da utilizzare. Un meccanismo può partecipare, per intero o parzialmente, alla realizzazione di una o più funzioni. Maggiore è la sensibilità dei dati, maggiore dovrà essere la robustezza del meccanismo che realizza le funzioni di sicurezza.

L'insieme delle funzioni di sicurezza rappresenta il sistema di protezione, esso è progettato in maniera da eliminare le vulnerabilità emerse in fase d'analisi, contrastando tutti i rischi cui il sistema è soggetto.

1.3 Normativa di riferimento

- D.Lgs. 29 luglio 2003 N. 196 Codice in materia di protezione dei dati personali e Disciplinare Tecnico in materia di misure minime di sicurezza;
- Legge nr. 547 del 23 dic. 1993 – "Reati informatici";
- Regio decreto 22 aprile 1941 n° 633, Integrato dal decreto legislativo n° 518 del 29 dicembre 1992 e successive modifiche per la protezione del diritto d'autore;
- Codice Civile – art. 2050;
- Direttiva 95/46/CE del parlamento Europeo e del Consiglio del 24 novembre 1995.

1.4 Definizioni

Sono definite di seguito le terminologie richiamate nel presente documento:

- Archivi: Archivi cartacei o informatici conservati presso l'ENPALS oggetto di trattamento da parte dello stesso.
- Trattamenti: Tutte e sole le operazioni (ad es: l'elaborazione, la modificazione, la conservazione, consultazione, la comunicazione, la diffusione, la cancellazione, etc. definite dall'art. 4, co. 1, lett. a del Codice) che l'ENPALS effettua sui dati degli interessati.
- Piattaforme: Elaboratori, sistemi automatizzati o strumenti per l'elaborazione e/o archiviazione dei dati o delle informazioni contenute negli archivi di cui sopra.
- Risorse: Tutti gli altri mezzi, a titolo esemplificativo la rete di trasmissione dati per il collegamento degli elaboratori, utilizzati per la corrente operatività.
- Locali: Locali, edifici, strutture logistiche dell'ENPALS che ospitano, anche temporaneamente, le Piattaforme e/o le Risorse necessarie all'operatività Amministrativa-Gestionale.

1.5 Revisioni

L'ENPALS si riserva la facoltà di modificare il presente documento ove le condizioni tecnico/organizzative e normative applicabili dovessero variare.
In particolare:

- ogni qualvolta dovessero cambiare le tecnologie e gli strumenti elettronici soggetti a protezione e misure di sicurezza;
- ad ogni controllo periodico cui le misure di sicurezza sono sottoposte per verificarne la validità ed efficacia;
- a seguito di variazioni della normativa applicabile.

2 Trattamenti dei dati svolti presso l'ENPALS (regola 19.1)

Per giungere alla efficace ed esaustiva compilazione del DPS è stata avviata preventivamente una ricognizione generale dei trattamenti svolti dall'ENPALS o affidati, in conformità alle prescrizione legislative, ad entità esterne.
Allo scopo sono state censite le banche dati, individuati i processi di lavoro negli uffici centrali e periferici, censite le misure di sicurezza per la protezione dei dati, individuati i soggetti fisici e giuridici che svolgono operazioni di trattamento dei dati e che sono abilitati a svolgerle, esaminate le deliberazioni in materia e le istruzioni normative interne che disciplinano l'operatività, osservati e classificati gli ambienti e i locali di lavoro nei quali avvengono i trattamenti.
L'analisi del ciclo di lavorazione dei dati ha riguardato sia i trattamenti svolti con strumenti elettronici, sia i trattamenti relativi ad atti e documenti cartacei.
Si è contemporaneamente proceduto ad una prima ricognizione dei rischi di distruzione e perdita dei dati (anche accidentale), di accessi non autorizzati, di trattamenti non consentiti o non conformi rispetto alle finalità della raccolta. Essi sono di seguito descritti unitamente alle misure individuate e adottate per ridurli al minimo.
Si precisa che la predetta ricognizione è stata prudentemente estesa, in via generale, a tutti i trattamenti, indipendentemente dalle circostanze operative che rendono necessario l'obbligo di compilazione del documento programmatico sulla sicurezza
Ai fini della rilevazione dei trattamenti cosi come previsto dal D.lgs 30 giugno 2003 "Codice in Materia di Protezione dei Dati Personali" (regola 19.1 dell'allegato B "Disciplinare Tecnico in Materia di Misure Minime di Sicurezza"), nel seguito viene indicato il censimento dei trattamenti effettuati e la rilevazione delle misure di sicurezza adottate.
Ai fini del D.lgs. 196/03 si intende:

- per **"trattamento"** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- per **"dato personale"** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- per **"dati identificativi"** i dati personali che permettono l'identificazione diretta dell'interessato;
- per **"dati sensibili"** i dati personali 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 o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- per **"dati giudiziari"** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

- Per **"strumenti elettronici"** gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

2.1 Rilevazione dei trattamenti

Nello schema che segue viene descritta sinteticamente la metodologia adottata ai fini delle rilevazioni delle informazioni utili alla completa ed esaustiva ricognizione dei trattamenti effettuati dall'ENPALS.
Partendo dai processi lavorativi svolti dalle diverse unità organizzative, sono state, in successione, individuate e classificate, secondo le previsioni di Legge, le basi dati di interesse ai fini della privacy.
Per ogni una di esse sono state rilevate le tecnologie sottese al trattamento e gli ambienti in cui le stesse sono localizzate al fine di individuare le misure di sicurezza tecniche implementate.
Le fasi finali del processo di rilevazione consistono nel porre in relazione le misure di sicurezza già presenti con i rischi considerati al fine di valutarne la loro adeguatezza e corrispondenza con quanto previsto dalla Legge.

Il risultato delle attività effettuate hanno consentito di ottenere un quadro esaustivo della situazione in essere e di poter procedere con gli adeguamenti urgenti delle misure ritenute inadeguate ovvero di pianificarne una loro implementazione nei termini consentiti dalla Legge.
L'approccio seguito, oltre a consentire l'individuazione dei singoli trattamenti, ha fornito le seguenti informazioni:

- soggetti che utilizzano o trattano i dati a diverso titolo, quali gli incaricati o soggetti terzi anche esterni all'ENPALS;
- ambito di comunicazione dei dati;
- responsabilità interne o esterne preposte al trattamento;
- modalità di trattamento elettronico e/o cartaceo;
- aree di localizzazione delle basi dati, locali in cui avvengono i trattamenti e meccanismi di sicurezza fisica implementati;
- le Strutture Centrali, relativamente ai processi primari, operano di norma sulla base dei dati forniti e gestiti dalle strutture periferiche di competenza.

Tali informazioni sono state ottenute attraverso l'utilizzazione dell'opera di rilevazione effettuata dai responsabili degli Uffici interessati, interviste effettuate ai diversi responsabili degli Uffici e materiale documentale già predisposto dall'ENPALS. Le tabelle compilate di tutte le notizie di cui sopra sono di seguito riportate:

Descrizione sintetica del trattamento		***Natura dei dati trattati***		***Struttura di riferimento***	***Altre strutture (anche esterne) che concorrono al trattamento***	***Descrizione degli strumenti utilizzati***
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
1. Trattamento pensionistico	Utente	X		DSIT	Direzione Prestazioni e Contributi	3270/web
2. Trattamento	Dipendenti	X	X	DSIT	Direzione	3270

giuridico del personale					Affari Generali e Personale	
3. Recupero Crediti	Dipendenti		X	DSIT	Direzione Contributi	web-protocollo https/accesso smart card
4. Stipendi	Dipendenti	X		DSIT	Direzione Affari Generali e Personale Data Management	Web protocollo https

2.2 Classificazione dei dati e obblighi di Notificazione

In relazione a quanto previsto dalla normativa vigente, vengono di seguito richiamati i trattamenti secondo la classificazione adottata dal documento di Notificazione come predisposto dall'Autorità Garante. Si precisa a tal proposito che la Notificazione prevede otto specifiche categorie di trattamenti, quali:

Tabella 1	Trattamento di dati genetici
Tabella 2	Trattamento di dati biometrici
Tabella 3	Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica
Tabella 4	Trattamento di dati idonei a rilevare lo stato di salute e la vita sessuale, trattati ai fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o a la fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria.
Tabella 5	Trattamento di dati idonei a rilevare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale
Tabella 6	Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi
Tabella 7	Trattamento di dati sensibili registrati in banche di dati a fine di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie
Tabella 8	Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischi sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni a comportamenti illeciti o fraudolenti.

A seguito delle ulteriori chiarificazioni del Garante intervenute con la Delibera n.1 del 31 marzo 2004 e con il chiarimento del 23 aprile 2004, l'ENPALS, non rientrando nella fattispecie dei trattamenti indicati dall'art.37, non ha provveduto, ad effettuare la

notificazione dei trattamenti all'Autorità Garante secondo le modalità previste dall'art.38 della Legge.

È stato inoltre verificato che per effetto dei trattamenti svolti, l'ENPALS non rientra nella casistica richiamata dall'art.39, comma 1, lettere a) e b), che prescrive l'obbligo di una specifica comunicazione da effettuarsi all'Autorità Garante ai fini autorizzativi.

2.3 Dati trattati

Oltre ai trattamenti come già indicati sopra, i dati trattati dall'ENPALS, classificati anche sulla base delle linee guida fornite dal Garante, sono riconducibili alle fattispecie indicate nella tabella che segue. Per alcuni di essi l'ENPALS opera un trattamento limitato alle finalità strettamente connesse alle proprie funzioni istituzionali e di corrente operatività interna.
Per questa categoria di dati, le finalità e modalità di trattamento, non prevedono l'obbligo di notificazione di cui all'art. 37 della Legge, ciò nonostante anche per essi vige l'obbligo di adozione delle misure di sicurezza a garanzia di tutela e riservatezza dei dati dell'interessato.

Nominativo, indirizzo ed altri elementi d'identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato e di lavoro, n. di telefono, di telefax, di posta elettronica, posizione rispetto agli obblighi militari, numero carta d'identità, passaporto, patente di guida, n. posizione previdenziale, targa automobilistica, dati fisici quali altezza e peso)
Codice fiscale e altri numeri d'identificazione personale (ad es. carte sanitarie)
Dati relativi alla famiglia e a situazioni personali (stato civile, minori a carico, consanguinei, altri appartenenti al nucleo famigliare)
Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione personale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae o lavorativo, competenze professionali, retribuzione, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente)
Attività economiche, commerciali, finanziarie e assicurative (dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni, identificativi finanziari, redditi, beni patrimoniali, investimenti, passività, solvibilità, prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi, dati assicurativi, dati previdenziali)
Dati relativi allo svolgimento di attività economiche e altre informazioni commerciali (es. fatturato, bilanci, aspetti economici, finanziari, organizzativi, produttivi, industriali, commerciali, imprenditoriali)
Istruzioni e cultura (curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audio-visivo, etc. - titoli di studio)
Beni, proprietà, possessi (proprietà, possessi e locazioni, beni e servizi forniti od ottenuti)
Convinzioni religiose, adesioni ad organizzazioni a carattere religioso
Adesione a partiti od organizzazioni a carattere politico
Stato di salute
Adesione a sindacati od organizzazioni a carattere sindacale

Informazioni concernenti taluni provvedimenti giudiziari

2.4 Categorie di interessati cui si riferiscono i dati

Le categorie di soggetti fisici e giuridici interessati a cui si riferiscono i dati, sono in dettaglio, le seguenti:

Personale dipendente e personale di altri enti pubblici in servizio presso ENPALS
Lavoratori autonomi e Parasubordinati
Candidati da considerare per l'instaurazione di un rapporto di lavoro
Consulenti e liberi professionisti, anche in forma associata
Aziende Contribuenti
Cittadini
Fornitori
Altri Soggetti od organismi pubblici
Familiari dell'interessato (per es. dipendenti)
Amministratori, Sindaci, Componenti degli Organi Collegiali e Componenti esterni dei Comitati

2.5 Finalità di trattamento

Le finalità del trattamento sono riconducibili alle seguenti macro-categorie:

- Finalità istituzionali
- Finalità amministrative e contabili
- Finalità di sicurezza e prevenzione dei reati.

2.6 Modalità di trattamento

I dati sono trattati sia in maniera automatizzata sia in forma cartacea.
Il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.
L'architettura del sistema informativo deputata ai trattamenti dell'ENPALS è basata su due piattaforme: i sistemi mainframe dell'INPS ed i sistemi di tipo servente installati presso la società EDS (che gestisce l'hosting nell'ambito del contratto quadro RUPA) e presso la DSIT. Tali piattaforme sono finalizzate a supportare le attività operative ed istituzionali dell'ENPALS ed all'automazione d'ufficio. La piattaforma tecnologica utilizzata è incentrata su sistemi MVS, MS/Windows, Linux, Microsoft Office per i sistemi distribuiti.
Le applicazioni sono basate sia su sistemi transazionali, Client/Server e tecnologia Web.

2.7 Ambito di comunicazione dei dati

Cittadini

Persone giuridiche, società di persone o di capitali, imprese individuali
Amministrazioni dello Stato
Altre amministrazioni ed enti pubblici
Organismi del servizio nazionale sanitario
Autorità giudiziaria
Organismi esteri ed internazionali

2.8 Esternalizzazione di trattamenti

Per lo svolgimento delle proprie attività e per quelle inerenti la gestione operativa interna, l'ENPALS affida l'elaborazione di alcune fasi di lavorazione dei dati a soggetti esterni.

Tali soggetti esterni dovranno operare con la qualificazione giuridica di Responsabili del Trattamento ai sensi dell'art.29 del D.Lgs.96/2003.

Insieme all'atto di conferimento dell'incarico alle società affidatarie del trattamento sono di norma impartite istruzioni su come proteggere le informazioni e richiesto un attestato di conformità alle disposizioni della Legge 196/03.

Periodicamente e ogni qualvolta se ne ravvisi la necessità, l'ENPALS, attraverso le proprie funzioni preposte, potrà effettuare interventi di verifica presso le società affidatarie dei trattamenti per appurare che vengano osservate le istruzioni impartite.

I soggetti esterni, nominati Responsabili del trattamento, con l'atto di nomina si impegneranno, anche contrattualmente, a fornire all'ENPALS tutte le informazioni e documentazioni tecniche ritenute necessarie.
Ai soggetti esterni, dovrà essere fatto assoluto divieto di affidare a ulteriori soggetti terzi, anche parzialmente, i trattamenti di cui l'ENPALS è Titolare.

2.9 Cifratura dei dati

In relazione alla Regola 19.8 del Disciplinare tecnico, l'ENPALS, per il normale svolgimento delle proprie funzioni istituzionali, non ricorre nell'obbligo di cifratura di dati riferiti in particolare alla sfera delle informazioni sanitarie degli interessati.

2.10 Diffusione dei dati

Nell'ambito delle proprie attività istituzionali, l'ENPALS non diffonde in alcuno modo dati.

2.11 Trattamento di dati via WEB

Il sito web istituzionale di ENPALS, oltre a fornire informazioni di carattere generale sull'Ente, eroga un insieme di servizi on-line, previa autorizzazione via PIN, che rappresentano l'interfaccia più innovativa tra l'Ente e i principali *stakeholders*: Cittadini, Aziende, Consulenti, Lavoratori Autonomi, Ispettori di Vigilanza.