

Copia di valutazione



Ordine degli Ingegneri della Provincia di Roma

Linee guida per la redazione del Documento Programmatico sulla Sicurezza (DPS)

Dott. Ing. Francesco Amendola

Dott. Ing. Gianluca Di Tomassi

Dott. Ing. Alessandro Masci

Data di pubblicazione: marzo 2006

© Tutti i diritti di traduzione, riproduzione, adattamento, duplicazione elettronica, stampa cartacea totale o parziale, sono riservati per tutti i Paesi. Nessuna parte di questa opera può essere riprodotta, registrata o trasmessa con qualsiasi mezzo, senza previa autorizzazione degli autori.

Copia di valutazione

Profilo degli autori

L'ing. Francesco Amendola si è laureato in Ingegneria Elettronica con Lode presso l'Università degli Studi di Roma Tre ed è un laureato del Collegio Universitario "Lamaro-Pozzani". Attualmente ricopre la carica di responsabile per la sicurezza della Nextel Italia s.r.l. e precedentemente è stato funzionario addetto alla sicurezza ICT ed alla protezione dei dati personali (D.Lgs. 196/03) presso la Pubblica Amministrazione. Ha inoltre conseguito il Master in "Tecniche di Management, Organizzazione e Gestione Aziendale" presso la Helyos Executive Master Management ed il Master di II livello in "Ingegneria ed Economia dell'Ambiente e del Territorio" presso l'Università degli Studi di Roma Tre. Si segnala, tra le esperienze professionali di maggior rilievo, l'attività di consulenza prestata presso uno dei maggiori player del mercato delle telecomunicazioni mobili di terza generazione (H3G s.p.a.).

L'Ing. Gianluca Di Tomassi è Ingegnere Informatico, laureato con il massimo dei voti presso dell'Università degli Studi di Roma Tre, con diploma di Master di II livello in "Economia e Tecnologia nella Società dell'Informazione". Svolge attività di Project leader e di consulenza in ambito privato e pubblico per primari clienti; esperto in project management, sistemi informativi intranet/internet, basi di dati e sicurezza informatica. È docente sulle tematiche relative a basi di dati e sistemi informativi, programmazione, progettazione di siti Web per molti corsi di formazione e riqualificazione del personale presso diversi enti e società (AIPA, Ministero del Lavoro e delle Politiche Sociali, Scuola Superiore della Pubblica Amministrazione, Engineering S.p.A., Business International, Alosys S.p.A., Sinter&Net, ecc.); ha inoltre prestato attività di docenza, in qualità di assistente, presso l'Università degli Studi Roma Tre nell'ambito del corso di Basi di Dati.

L'Ing. Alessandro Masci è Ingegnere Informatico, laureato con lode presso l'Università degli Studi di Roma "La Sapienza", con diploma di Master di II livello in "Economia e Tecnologia nella Società dell'Informazione". Svolge attività di responsabile per l'area Sistemi ed Applicazioni dell'Università degli Studi di Roma Tre.

È esperto su tematiche relative alle basi di dati, sistemi operativi e sicurezza informatica, applicazioni web-oriented, servizi di rete; ha svolto inoltre docenze su tematiche relative alle basi di dati e sistemi informativi, programmazione e progettazione di siti Web.

Profilo del revisore

L'ing. Christiam Salvatori si è laureato in Ingegneria Elettronica presso l'Università degli Studi di Bologna effettuando la sua tesi di laurea presso il laboratorio di ricerca francese del LIRMM (Laboratoire d'Informatique de Robotique et de Microelectronique de Montpellier).

La sua esperienza nell'ambito ICT spazia da sistemi informativi quali sistemi di gestione di rete, di apparati, di controllo e di OSS utilizzati in ambienti complessi quali operatori TLC come Telecom Italia, Deutsche Telekom. Ha maturato una esperienza sia tecnica che manageriale, in ambienti lavorativi internazionali (avendo trascorso 5 anni in UK e 7 mesi in Germania) nel settore ICT. Svolge attività di consulenza presso il Dipartimento della Protezione Civile ed in Filas (per quanto riguarda il trasferimento di innovazione tecnologica verso le PMI) ed è un Partner della TransTec Services S.r.l.. Ha inoltre svolto attività di consulenza presso Telcordia Technologies, Granite Systems, Syndesis, società Nord Americane attive nell'area degli Operations Support Systems. Ha infine lavorato presso Global Crossing, Alcatel, Sirti e Trion Präzisionselektronik.

Indice

1 INTRODUZIONE.....	3
1.1 CONTESTO NORMATIVO DI RIFERIMENTO.....	3
1.2 DESTINATARI DELLA MONOGRAFIA.....	5
1.3 ORGANIZZAZIONE DELLA MONOGRAFIA.....	6
PARTE I.....	7
2 IL DECRETO LEGISLATIVO 196/2003, ALIAS CODICE PRIVACY.....	8
2.1 ADEMPIMENTI NORMATIVI.....	8
2.2 LA CULTURA DELLA SICUREZZA COME VANTAGGIO COMPETITIVO	10
2.3 MISURE DI SICUREZZA.....	12
2.3.1 Sistema di autenticazione informatica.....	13
2.3.2 Sistema di autorizzazione.....	14
2.3.3 Ulteriori misure di sicurezza.....	14
2.3.4 Documento Programmatico sulla Sicurezza.....	15
2.3.5 Tutela e garanzia in caso di consulenze esterne	17
2.3.6 Misure di sicurezza idonee.....	17
2.4 PROFILI DI RESPONSABILITÀ.....	18
2.4.1 Profili di responsabilità civile.....	18
2.4.2 Profili di responsabilità amministrativa.....	18
2.4.3 Profili di responsabilità penale.....	19
PARTE II.....	20
3 REDAZIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA.....	21
3.1 ARTICOLAZIONE DEL DOCUMENTO.....	21
3.2 ELENCO DEI TRATTAMENTI DI DATI PERSONALI (REG. 19.1 - ALL. B).....	23
3.2.1 Tipologie di analisi.....	23
3.2.2 Informazioni essenziali.....	25
3.2.3 Ulteriori elementi per descrivere gli strumenti.....	27
3.2.4 Esempio di elenco dei trattamenti effettuati.....	28
3.3 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ (REG. 19.2 - ALL. B).....	32
3.3.1 Informazioni essenziali.....	32
3.3.2 Esempio di distribuzione dei compiti e delle responsabilità.....	33
3.3.3 Responsabili ed incaricati al trattamento di dati personali.....	36
3.3.4 Esempio di individuazione dei responsabili e degli incaricati	36
3.4 ANALISI DEI RISCHI E DELLE CONTROMISURE (REG. 19.3 - ALL. B).....	37
3.4.1 Introduzione all'analisi del rischio.....	37
3.4.2 Metodologia di analisi del rischio di tipo quantitativo.....	38
3.4.3 Metodologia di analisi del rischio di tipo qualitativo.....	39
3.4.4 Esempio di metodologia di analisi del rischio.....	39
3.4.5 Metodologia di analisi del rischio mista.....	40

Copia di valutazione

3.4.6	Interventi correttivi.....	41
3.4.7	Informazioni essenziali.....	42
3.4.8	Esempio di analisi dei rischi che incombono sui dati.....	44
3.5	MISURE IN ESSERE E DA ADOTTARE (REG. 19.4 - ALL. B).....	46
3.5.1	Informazioni essenziali.....	46
3.5.2	Ulteriori elementi per la descrizione analitica delle misure di sicurezza.....	47
3.5.3	Piano degli interventi.....	49
3.5.4	Esempio di misure di sicurezza in essere o da adottare.....	50
3.6	CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI (REG. 19.5 - ALL. B).....	52
3.6.1	Informazioni essenziali.....	52
3.6.2	Ulteriori elementi relativi alle modalità di salvataggio e ripristino dei dati.....	53
3.6.3	Esempio sulle modalità di salvataggio e ripristino dei dati.....	55
3.7	PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI (REG. 19.6 - ALL. B).....	58
3.7.1	Informazioni essenziali.....	58
3.7.2	Esempio di pianificazione degli interventi formativi.....	59
3.8	TRATTAMENTI DI DATI AFFIDATI ALL'ESTERNO (REG. 19.7 - ALL. B).....	61
3.8.1	Informazioni essenziali.....	61
3.8.2	Esempio di trattamenti affidati all'esterno.....	62
3.9	CIFRATURA DEI DATI O SEPARAZIONE DEI DATI IDENTIFICATIVI (REG. 19.8 - ALL. B).....	64
3.9.1	Informazioni essenziali.....	64
3.9.2	Esempio di cifratura dei dati o separazione dei dati identificativi.....	65
PARTE III.....		66
4 COSTI E FIGURE PROFESSIONALI.....		67
4.1	I PARAMETRI DI RIFERIMENTO.....	67
4.2	LE FIGURE PROFESSIONALI.....	68
4.3	LE ATTIVITÀ DI REDAZIONE DEL DPS.....	70
4.4	COSTI PER LA REALIZZAZIONE DEGLI INTERVENTI.....	71
4.5	LO SCHEMA DI DETERMINAZIONE DEI COSTI.....	71
4.5.1	Parametro di moltiplicazione	74
APPENDICE.....		76
5 ALLEGATI.....		77
5.1	MISURE MINIME DI SICUREZZA.....	77
5.2	CHECK LIST DELLE CONTROMISURE.....	81
5.3	LETTERE DI INCARICO.....	89
5.3.1	Fac-Simile di lettera per la nomina individuale a “responsabile” del trattamento.....	89
5.3.2	Fac-Simile di lettera per la nomina individuale ad “incaricato” del trattamento.....	91
5.3.3	Fac-Simile di lettera per le istruzioni agli Incaricati del trattamento dei dati.....	92
5.4	GLOSSARIO.....	95



1 INTRODUZIONE

Il 1 Gennaio 2004 è entrato in vigore in Italia il “*Codice in materia di protezione dei dati personali*” (Decreto Legislativo n. 196 del 30/6/2003) che riforma interamente la disciplina sulla *privacy* intesa appunto come “*diritto alla protezione dei dati personali*”, ex art. 1. Detto codice, abrogando e sostituendo tutte le leggi, i decreti ed i regolamenti pre-vigenti nel medesimo ambito di applicazione, fermo restando ex art. 184, comma 3, “*le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi*”, riunisce in un testo unico ed in un contesto organico l’intera normativa in materia di *privacy*.

1.1 CONTESTO NORMATIVO DI RIFERIMENTO

L’art. 2 del D.Lgs. 196/03 esplica le finalità del codice, individuandole nella garanzia che “*il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali*”; inoltre, nel comma 2, afferma anche che il trattamento dei dati personali deve avvenire “*assicurando un elevato livello di tutela dei diritti e delle libertà*” dell’interessato dal trattamento, “*nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l’adempimento degli obblighi da parte dei titolari del trattamento*”.

Il codice individua dunque, nell’art. 5, il suo ambito di applicazione in tutti i trattamenti di dati personali effettuati “*da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato*”; per quanto appena affermato, senza alcuna pretesa di esaustività, tutte le organizzazioni pubbliche e private, gli enti economici e non economici, le strutture sanitarie, i soggetti privati che trattano dati personali “*destinati ad una comunicazione sistematica o alla diffusione*” (comma 3) sono tenuti a rispettare la nuova normativa, la cui corretta applicazione va ben oltre l’adempimento formale degli obblighi giuridici, bensì consente di migliorare l’organizzazione e la gestione aziendale, i processi e gli standard di lavoro, non ultimi la qualità e la rispondenza dei risultati.

Copia di valutazione

Operativamente, al fine di garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati da una qualsiasi organizzazione, il codice prevede l'adozione di un insieme di misure minime di sicurezza, intese ex art. 4, comma 3, lettera a), come complesso di *“misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti”*. Di fatto l'intero processo di adeguamento può configurarsi come l'adozione di un vero e proprio sistema di gestione della sicurezza dei dati trattati.

Tra le misure minime così come riportate nell'art. 34 del codice, è prevista la redazione di un documento che riporti la pianificazione degli interventi da attuare, per superare le criticità presenti nell'intero sistema informativo: questo documento è pertanto detto “Documento Programmatico sulla Sicurezza”, ovvero DPS, e sarà oggetto di una trattazione approfondita in questo testo.

Riguardo l'obbligo e la modalità di redazione di tale documento non esiste al momento una dottrina definitiva, fermo restando che dall'organo Garante per la protezione dei dati personali sono state emesse delle linee guida chiarificatrici. La posizione condivisa dagli autori prevede che il DPS vada redatto comunque da tutti coloro che effettuano un trattamento di dati personali, in quanto esso è un utilissimo strumento di autoanalisi che, per quanto già accennato in precedenza, non si giustifica soltanto come un obbligo formale della vigente normativa in materia, bensì si configura come un valido ausilio all'individuazione delle fonti di rischio, alla loro classificazione in base alla gravità dell'impatto che possono produrre, alla pianificazione temporale delle priorità di intervento per l'abbattimento, o quanto meno il controllo, dei fattori di rischio ritenuti maggiormente nocivi per le attività svolte.

Se, ad ogni modo, si vuole individuare un obbligo è possibile ragionevolmente pensare che il DPS debba essere redatto, a partire dal 31 Marzo 2006, soltanto da coloro che trattano dati sensibili e giudiziari tramite strumenti elettronici, con cadenza annuale entro il 31 Marzo; allo stato attuale quest'obbligo riguarda invece solo i titolari del trattamento dei dati sensibili o relativi ai provvedimenti di cui all'articolo 686 del codice di procedura penale, effettuato tramite elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.

Tuttavia si ribadisce come lo strumento Documento Programmatico sulla Sicurezza non debba essere visto come un mero adempimento normativo, bensì come un valido mezzo per gestire e controllare meglio il proprio sistema informativo e dunque, in quest'ottica, è auspicabile e

Copia di valutazione

consigliato che venga redatto anche da chi si sente escluso dall'ambito di applicazione del D.Lgs. 196/03.

Infine la mancata adozione delle misure minime di sicurezza rende penalmente perseguibili gli inadempienti, ovvero chiunque essendovi tenuto omette di adottarle, i quali possono essere puniti, ex art. 169, “*con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro*”, salvo l'adozione di un ravvedimento operoso: in aggiunta a ciò l'art. 15 del codice prevede che “*chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*”, assimilando le responsabilità di trattamento a quelle imputabili a coloro che svolgono attività pericolosa: in pratico questo implica principalmente che l'onere della prova ricade su colui che genera l'evento dannoso, ritenuto responsabile a meno che non provi di avere adottato tutte le misure idonee ad evitare il danno.

Dunque l'adozione delle misure minime di sicurezza solleva il titolare del trattamento da responsabilità penali, ma ciò potrebbe non essere sufficiente per evitare danni per effetto del trattamento e dunque responsabilità civili: infatti, oltre le misure minime, dovrebbe intervenire la diligenza del titolare che, in relazione all'evoluzione tecnica ed all'esperienza maturata nel settore, lo porterà ad adottare ulteriori misure, appunto idonee, che siano in grado di garantire una maggiore efficacia nella riduzione dei rischi derivanti da un incauto trattamento.

Per quanto fin qui riportato, si chiarisce come questo monografia miri a fornire uno strumento di ausilio alla redazione e/o all'aggiornamento del DPS, in particolar modo per organizzazioni di piccole e medie dimensioni, in linea con le linee guida operative emanate dal Garante per la protezione dei dati personali.

1.2 DESTINATARI DELLA MONOGRAFIA

La monografia, nascendo in seno all'Ordine degli Ingegneri della provincia di Roma, ha come pubblico di riferimento preferenziale tutti gli ingegneri che operano nel campo dell'ICT, con particolare riguardo verso coloro che svolgono attività di gestione, adeguamento e controllo dei sistemi informativi, nell'ottica di implementare un sistema di gestione della sicurezza dei dati oggetto di trattamento.

Pertanto essa non vuole essere un manuale d'esempio per la redazione del DPS, bensì si configura più propriamente come una linea guida (*best practices*) da seguire nell'adozione di tutte le misure minime di sicurezza finalizzate ad una corretta gestione del rischio in relazione al sistema



informativo da proteggere, che sia di riferimento per tutti quei professionisti che già operano o che si troveranno ad operare nell'ambito di applicazione del D.Lgs. 196/03.

1.3 ORGANIZZAZIONE DELLA MONOGRAFIA

La redazione di questa monografia è stata suddivisa in tre parti, di seguito dettagliate:

- la prima parte contiene informazioni di carattere generale sul ”*Codice in materia di protezione dei dati personali*“ e sulle opportunità, in termini di vantaggio competitivo, che l'applicazione di tale codice può portare a qualsiasi organizzazione, sia essa di natura pubblica sia privata, che si trovi ad adottarlo;
- la seconda parte contiene le linee guida, ovvero le *best practices*, sulla redazione del DPS, così come previste implicitamente nel codice stesso e successivamente esplicitate dal Garante per la protezione dei dati personali, opportunamente corredate con esempi, osservazioni e indicazioni per la corretta stesura del documento programmatico;
- infine la terza parte contiene il piano tariffario relativo alle differenti tipologie di prestazioni professionali che l'ingegnere si può trovare ad erogare; naturalmente, dal momento che le realtà di interesse possono essere piuttosto eterogenee, occorre fare attenzione ed utilizzare con la dovuta cautela le formule predisposte.