Documento Programmatico sulla Sicurezza

(Redatto secondo le disposizioni dell'Articolo 34 e della regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali - D.Lgs. 196/03).

INDICE

PARTE QUINTA
MISURE DA ADOTTARE PER LA PROTEZIONE DELLE AREE E DEI LOCALI RILEVANTI AI FINI DELLA LORO CUSTODIA ED ACCESSIBILITA'

PARTE SESTA
FORMAZIONE DEGLI INCARICATI DEL TRTTAMENTO

PARTE SETTIMA
CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DI MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

PARTE OTTAVA
PERIODICITA' DI REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

PARTE PRIMA

IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

1.1 Revisione

Indice delle revisioni

Revisione	Data	Descrizione	Redatto	Verificato	Approvato

1.2 Scopo

Il presente Documento Programmatico per la Sicurezza (infra, per comodità «DPS») rappresenta il riferimento per tutte le misure di sicurezza adottate per un trattamento dei dati personali, conforme a quanto previsto dal CODICE IN MATERIA DI DATI PERSONALI - infra, per comodità «CODICE» [D.Lgs. 196/03 pubblicato in Gazzetta Ufficiale il 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 1231L].

Obiettivo del DPS è, secondo la logica dell'art. 31 del CODICE, costituire la guida per quanto fatto e programmato al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta mediante l'adozione di misure di sicurezza quale insieme degli accorgimenti tecnici, informatici, organizzativi, logistici, fisici procedurali di sicurezza.

Tutti i documenti citati nel DPS e quelli riassunti nell'«Elenco Allegati» formano parte integrante del DPS.

Il DPS è pubblicato all'interno della struttura Titolare del Trattamento e riservato nei confronti di terzi.

Al fine di dare idonea visibilità a tutti i soggetti, a vario titolo incaricati, una copia del CODICE viene conservata e resa disponibile a chiunque ne faccia richiesta.

1.3. Definizioni (art. 4).

Trattamento: qualunque operazione, o complesso di operazioni, effettuata anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, registrazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

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.

Dati sensibili: i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, le adesioni a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute o la vita sessuale.

Dati giudiziari: i dati personali idonei a rilevare i provvedimenti di cui all'art. 3,comma 1, lettere da a) ad o) e da r) ad u), del D.P.R. 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 artt. 60 e 61 c.p.p.

Titolare: la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alla finalità, alle modalità del trattamento, di dati personali e agli strumenti utilizzati ivi compreso il profilo della sicurezza.

Responsabile: la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano legate ad un abbonato o utente ricevente , identificato o identificabile.

Misure minime: il complesso delle informazioni tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art.31.

Strumenti elettronici: gli elaboratori, i programmi per gli elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione: i dati o i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave: componente di un credenziale di autenticazione associata ad una persona e da questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

PARTE SECONDA

RUOLI, COMPITI E NOMINA DELLE PERSONE PREVISTE PER LA SICUREZZA DEI DATI PERSONALI

Questa sezione, comprensiva dei dati in essa richiamati, riporta, in conformità di quanto previsto dalla regola 19.2 dell'Allegato B al D.Lgs.196/03, la distribuzione dei compiti e delle responsabilità all'interno della struttura titolare del trattamento.

2.1 Titolare del trattamento dei dati personali.

Il Titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali a agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento deve assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del CODICE e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (infra DISCIPLINARE) tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il Titolare del trattamento, in relazione all'attività svolta, può, se lo ritiene opportuno, nominare, incaricandoli per iscritto, uno o più Responsabili del trattamento dei dati che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del CODICE e del DISCIPLINARE. Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile del trattamento dei dati, ne assumerà tutte le responsabilità e funzioni.

I Responsabili del trattamento possono essere interni o esterni alla struttura del Titolare.

In caso di Responsabili del trattamento esterni, la lettera di incarico individua le modalità del trattamento, le finalità e le banche dati oggetto del trattamento.

2.2 Il Responsabile del trattamento dei dati personali.

I) Compiti.

Il Responsabile del trattamento dei dati personali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti:

- garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- redigere ed aggiornare l'elenco delle sedi in cui vengono trattati i dati;
- redigere ed aggiornare l'elenco degli uffici in cui vengono trattati i dati;
- redigere ed aggiornare l'elenco delle banche dati oggetto di trattamento;
- se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare l'elenco dei sistemi di elaborazione;
- definire e successivamente verificare, con cadenza semestrale, le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locai, rilevanti ai fini della loro custodia ed accessibilità come specificato in seguito;

- qualora il trattamento dei dati sia stato affidato, in tutto o in parte, all'esterno della struttura del titolare, controllare e garantire che tutte le misure di sicurezza, riguardanti i dati personali, siano applicate;
- custodire e conservare i supporti utilizzati per la copia dei dati;
- se il trattamento è effettuato con strumenti informatici individuare, nominare ed incaricare per iscritto:
    - uno o più Responsabili della gestione e della manutenzione degli strumenti informatici;
    - uno o più Incaricati della custodia delle copie delle credenziali;
    - uno o più Incaricati delle copie di sicurezza delle banche dati.

Il Responsabile del trattamento individua per ogni banca dati oggetto del trattamento, identificandoli nominativamente o per categorie omogenee, gli Incaricati del trattamento dei dati personali, impartendo loro istruzioni adeguate affinché il trattamento sia effettuato nei termini e nei modi stabiliti dal CODICE e sorvegliando la reale applicazione di quanto stabilito.

Periodicamente, e comunque almeno annualmente, verifica la sussistenza per le condizioni per la conservazione dei profili di autorizzazione degli Incaricati del trattamento dei dati personali.

Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile del trattamento dei dati personali, egli ne assume tutte le responsabilità e funzioni.

II) Nomina.

La nomina di ciascun Responsabile del trattamento dei dati personali interno, viene effettuata dal Titolare del trattamento con una lettera di incarico, in cui sono specificate le responsabilità che gli sono affidate, controfirmata dall'interessato per accettazione.

Il Titolare del trattamento informa ciascun Responsabile del trattamento dei dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalla normativa in vigore.

La nomina del Responsabile del trattamento dei dati personali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile del trattamento dei dati personali può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

2.3 Il Responsabile della gestione e della manutenzione degli strumenti elettronici.

I) Compiti.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di Banche dati.

Il Responsabile del trattamento dei dati, in relazione all'attività svolta, individua, nomina ed incarica per iscritto, uno o più se lo ritiene opportuno, Responsabili della gestione e della manutenzione degli strumenti elettronici.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici sovrintende alla:

- attivazione delle credenziali di autenticazione agli Incaricati del trattamento, su indicazione del Responsabile del trattamento, per tutti i trattamenti effettuati con strumenti informatici;
- definizione delle politiche da adottare per la protezione dei sistemi contro i rischi di violazione del informativo, verificandone l'efficacia con cadenza almeno semestrale;
- informa il Responsabile del trattamento dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il Responsabile del trattamento dei dati personali ritenga di non nominare alcun Responsabile della gestione e della manutenzione degli strumenti elettronici, ne assumerà tutte le responsabilità e funzioni.

II) Nomina.

Il Responsabile del trattamento dei dati personali nomina uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici, specificando gli elaboratori e le banche dati cui è chiamato a sovrintendere.

La nomina di uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici viene effettuato con una con una lettera di incarico controfirmata per accettazione.

La nomina dei Responsabili della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dei Responsabili della gestione e della manutenzione degli strumenti elettronici può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso, ed affidata eventualmente ad altro soggetto.

2.4 L'Incaricato della custodia delle copie delle credenziali.

I) Compiti.

Il Responsabile del trattamento dei dati personali, in relazione all'attività svolta, individua, nomina ed incarica per iscritto, se lo ritiene opportuno, uno o più Incaricati della custodia delle copie delle credenziali.

E' compito degli Incaricati della custodia delle copie delle credenziali:

- gestire e custodire le credenziali per l'accesso ai dati degli Incaricati del trattamento;
- predisporre, per ogni Incaricato del trattamento una busta sulla quale è indicato il nome dell'incaricato e all'interno della quale deve essere indicata la credenziale usata. Le buste con le credenziali devono essere conservate in luogo chiuso e protetto;
- istruire gli Incaricati del trattamento sull'uso delle parole chiave, e sulle caratteristiche che devono avere, e sulle modalità per la loro modifica in autonomia;

Inoltre, a seguito di quanto disposto dal Responsabile del trattamento in relazione agli Incaricati del trattamento:

- revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali;

- revocare le credenziali per l'accesso ai dati degli Incaricati del trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi.

Qualora il Responsabile del trattamento dei dati personali ritenga di non nominare alcun Incaricato della custodia delle copie delle credenziali, ne assumerà tutte le responsabilità e funzioni.

II) Nomina.

La nomina di uno o più Incaricati della custodia delle copie delle credenziali viene effettuato con una con una lettera di incarico controfirmata per accettazione.

La nomina dei Incaricati della custodia delle copie delle credenziali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dei Incaricati della custodia delle copie delle credenziali può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso, ed affidata eventualmente ad altro soggetto.

2.5 L'Incaricato delle copie di sicurezza delle banche dati.

I) Compiti.

L'Incaricato delle copie della sicurezza delle banche dati è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che ha il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

E' onere del Responsabile del trattamento dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati delle copie della sicurezza delle banche dati.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce, con il supporto tecnico del Responsabili della gestione e della manutenzione degli strumenti elettronici la periodicità con cui devono essere effettuate le copie di sicurezza delle Banche di dati trattate.

I criteri devono essere concordati con il Responsabili della gestione e della manutenzione degli strumenti elettronici in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni Banca di dati devono essere definite le seguenti specifiche:

- il «Tipo di supporto» da utilizzare per le «Copie di Back-Up»;
- il numero di «Copie di Back-Up» effettuate ogni volta;
- se i supporti utilizzati per le «Copie di Back-Up» sono riutilizzati ed in questo caso con quale periodicità;
- se per effettuare le «Copie di Back-Up» si utilizzano procedure automatizzate e programmate;
- le modalità di controllo delle «Copie di Back-Up»;
- la durata massima stimata, di conservazione delle informazioni, senza che ci siano perdite o cancellazione di dati;
- l'Incaricato del trattamento a cui è assegnato il compito di effettuare le «Copie di Back-Up»;
- le istruzioni e i comandi necessari per effettuare le «Copie di Back-Up».

E' compito degli Incaricati delle copie della sicurezza delle banche dati:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Responsabile del trattamento dei dati personali;
- assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro;
- assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato;
- di provvedere a conservare, con la massima cura e custodia, i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di persone non autorizzate;
- di segnalare tempestivamente al Responsabili della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il Responsabile del trattamento dei dati personali ritenga di non nominare alcun Incaricato delle copie della sicurezza delle banche dati, ne assumerà tutte le responsabilità e funzioni.

II) Nomina.

Anche se non espressamente previsto dalla norma, è opportuno che il Responsabile del trattamento dei dati personali nomini uno o più Incaricati delle copie di sicurezza delle banche dati, specificando gli elaboratori e le banche dati che è chiamato a sovrintendere.

La nomina di uno o più Incaricati delle copie di sicurezza delle banche dati deve essere effettuata con una lettera di incarico e deve essere controfirmata per accettazione.

2.6 Incaricato del trattamento dei dati personali.

I) Compiti.

Gli Incaricati del trattamento sono le persone fisiche, autorizzate dal Responsabile del trattamento, a compiere operazioni di trattamento sui dati personali.

Gli Incaricati del trattamento dei dati personali devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli Incaricati del trattamento dei dati personali, qualora trattino dati personali con l'ausilio di strumenti elettronici, deve essere assegnata una parola chiave ed un codice di autenticazione informatica.

Agli Incaricati del trattamento dei dati personali è prescritto di adottare le necessarie cautele per assicurare la sicurezza della parola chiave e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato. In particolare:

- la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la parola chiave non deve contenere riferimenti riconducibili facilmente all'incaricato;

- l'Incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi;
- in caso di trattamento di dati sensibili o di dati giudiziari, la parola chiave deve essere modificata almeno ogni tre mesi;
- gli Incaricati del trattamento non devono in nessun caso lasciare incustodito e accessibili lo strumento elettronico, durante una sessione di trattamento di dati personali;
- gli Incaricati del trattamento devono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e documenti contenenti dati personali;
- quando gli atti contenenti dati sensibili o giudiziari sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

II) Nomina.

La nomina di ciascun Incaricato del trattamento dei dati personali deve essere effettuata dal Responsabile del trattamento con una o più lettere di incarico in cui sono specificati i compiti che gli sono stati affidati e l'accesso alle banche di dati.

La nomina dell'Incaricato del trattamento dei dati personali è a tempo indeterminato e decade per revoca o dimissioni dello stesso.

La nomina dell'Incaricato del trattamento dei dati personali può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati senza preavviso, ed eventualmente affidata ad un altro soggetto.

PARTE TERZA

ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

Negli allegati citati in questa sezione, secondo quanto previsto dalla regola 19.1 dell'Allegato B al CODICE, viene riportato l'elenco dei trattamenti effettuati dal titolare, direttamente o tramite affidamento a terzi esterni, con l'indicazione per ciascun trattamento di:

- descrizione del trattamento di dati;
- natura dei dati trattati: comuni, sensibili, giudiziari;
- Struttura di riferimento (indicazione della riferibilità del trattamento alla struttura nel suo insieme o a singole sotto-strutture o funzioni, Es.: personale, contabilità, etc.);
- l'identificazione della banca dati (data base, archivio informatico, data base riferibili ad applicativi, gruppi di file non organizzati);
- ubicazione fisica dei supporti di memorizzazione (localizzazione fisica dell'elaboratore sui cui dischi sono memorizzati i dati).

PARTE QUARTA

ANALISI DEL RISCHIO DI TRATTAMENTO NON CONFORME - MISURE DI SICUREZZA ADOTTATE

Questa sezione contiene, ai sensi delle Regole 19.3 e 19.4 dell'Allegato B del CODICE, ed alla luce dei rischi gravanti sui dati e relativi all'accesso di soggetti interni ed esterni non legittimati ed alla distruzione o cancellazione (anche involontaria) di dati, le misure di sicurezza, minime e/o idonee, poste in essere dalla struttura che effettua il trattamento.

4.1 Trattamenti con l'ausilio di strumenti elettronici.

A. Sistema di autenticazione informatica.

I) Procedura di identificazione.

Il trattamento è consentito solamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ad uno specifico trattamento o ad un insieme di trattamenti.

II) Identificazione dell'incaricato.

Il Responsabile del trattamento dei dati personali si assicura che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli incaricati dotati di una o più credenziali di autenticazione individuate tra le seguenti:

- un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata, conosciuta solamente dal medesimo;
- un dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato, eventualmente associato ad un codice identificativo o ad una parola chiave;
- una caratteristica biometria dell'incaricato, eventualmente associata ad un codice identificativo o ad una parola chiave.

Il Responsabile del trattamento dei dati personali si assicura che il medesimo codice per l'identificazione non sia assegnato ad altri incaricati, neppure in tempi diversi.

Il Responsabile del trattamento dei dati personali si assicura che le credenziali di autenticazione non utilizzate da almeno 6 (sei) mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Il Responsabile del trattamento dei dati personali si assicura che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni Incaricato del trattamento possono essere assegnate, od associate individualmente, una o più credenziali di autenticazione.

III) Caratteristiche della parola chiave.

Gli incaricati vengono istruiti sull'utilizzo della parola chiave, quando è prevista dal sistema di autenticazione:

- deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- non deve contenere riferimenti agevolmente riconducibili all'incaricato;
- deve essere modificata dall'Incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni 6 (sei) mesi (tre mesi in caso di trattamento di dati sensibili e/o giudiziari).

IV) Cautele per assicurare la segretezza della componente riservata della credenziale.

Gli incaricati devono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che è stato loro affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, etc.). In particolare, è fatto divieto di comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico.

V) Istruzioni per non lasciare incustodito ed accessibile lo strumento elettronico.

Gli incaricati hanno l'obbligo di:

- non lasciare incustodito il proprio posto di lavoro;
- di chiudere tutte le applicazioni aperte, o meglio ancora di spegnere il sistema informatico, in caso di assenza prolungata.

VI) Accesso straordinario.

Gli Incaricati della custodia delle copie delle credenziali, hanno il compito di assicurare la disponibilità dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

Gli Incaricati della custodia delle copie delle credenziali devono informare tempestivamente l'Incaricato del trattamento ogni qualvolta sia effettuato un tale tipo di intervento.

B. Sistema di autorizzazione.

I Responsabili del trattamento individuano, nominalmente o per categorie omogenee, quali Incaricati del trattamento possono avere accesso ad ogni singola banca di dati personali o tipologia di dati personali trattata.

In particolare ad ogni Incaricato del trattamento può essere data, dal Responsabile del trattamento, la possibilità di:

- Inserire nuove informazioni nella banca di dati personali;
- Accedere alle informazioni di visualizzazione e stampa;
- Modificare le informazioni esistenti nella banca di dati personali;
- Cancellare le informazioni esistenti nella banca di dati personali.

I) Altre istruzioni destinate agli incaricati del trattamento.

In considerazione di quanto disposto dal CODICE, è fatto divieto a chiunque di:

- effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del trattamento dei dati personali di dati oggetto del trattamento;
- effettuare copie fotostatiche, o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- sottrarre, cancellare, distruggere, senza l'autorizzazione del Responsabile del trattamento dei dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;

- consegnare a persone non autorizzate dal Responsabile del trattamento dei dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

II) Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni.

Il Responsabile del trattamento dei dati personali ha il compito di verificare periodicamente le credenziali di autenticazione e di aggiornare l'elenco dei soggetti autorizzati al trattamento dei dati.

C. Manutenzione dei sistemi di elaborazione dei dati.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici, anche avvalendosi di consulenti interni o esterni, verifica ogni anno:

- la situazione delle apparecchiature hardware istallate con cui vengono trattati i dati;
- la situazione delle apparecchiature periferiche;
- la situazione dei dispositivi di collegamento con le reti pubbliche. La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:
    - la sicurezza dei dati trattati;
    - il rischio di distruzione o di perdita;
    - il rischio di accesso non autorizzato o non consentito.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici deve aggiornare il Report annuale dei rischi hardware conformemente al modulo.

I Responsabili della gestione e della manutenzione degli strumenti elettronici, nel caso in cui esistano rischi evidenti, devono informare il Responsabile del trattamento dei dati personali perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

D. Manutenzione dei sistemi operativi e dei software istallati.

Al Responsabile della gestione e della manutenzione degli strumenti elettronici è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software istallate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- la sicurezza dei dati trattati;
- il rischio di distruzione o di perdita;
- il rischio di accesso non autorizzato o non consentito.

Tenendo conto, in particolare, di:

- disponibilità di nuove versioni migliorative dei software utilizzate;
- segnalazioni di Patch, Fix, o Service-Pack per la rimozione di errori o malfunzionamenti;
- segnalazioni di Patch, Fix, o Service-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici deve aggiornare il Report annuale dei rischi sui software istallati conformemente al modulo.

I Responsabili della gestione e della manutenzione degli strumenti elettronici, nel caso in cui esistano rischi evidenti, devono informare il Responsabile del trattamento dei dati personali affinché siano presi gli opportuni provvedimenti per assicurare il trattamento di dati in conformità delle norme in vigore.

E. Misure da adottare per garantire l'integrità e la disponibilità dei dati.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui devono essere effettuate le copie di sicurezza delle banche di dati trattati.

I criteri vengono definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici, per ogni banca di dati deve predisporre le istruzioni di copia, verifica e ripristino dei dati, utilizzando il modulo.

Il "Documento con le istruzioni di copia" deve essere conservato a cura del Responsabile del trattamento dei dati personali in luogo sicuro e deve essere trasmesso in copia controllata a ciascun Incaricato delle copie di sicurezza delle banche dati.

In particolare per ogni banca di dati devono essere stabilite le seguenti specifiche:

- il tipo di supporto da utilizzare per le Copie di sicurezza dei dati;
- il numero di Copie di sicurezza dei dati effettuate ogni volta;
- se i supporti utilizzati per le Copie di sicurezza dei dati sono riutilizzati ed in questo caso con quale periodicità;
- se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate;
- le modalità di controllo delle Copie di sicurezza dei dati;
- la durata massima stimata di conservazione e delle informazioni senza che ci siano perdite o cancellazione dei dati;
- il nome dell'incaricato a cui è stato affidato il compito di effettuare le Copie di sicurezza dei dati;
- le istruzioni ed i comandi necessari per effettuare le Copie di sicurezza dei dati;
- le istruzioni ed i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

Al Responsabile del trattamento dei dati personali è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le Copie di sicurezza delle banche di dati trattate, in funzione anche delle eventuali opportunità offerte dall'evoluzione tecnologica, utilizzando il modulo.

F. Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Il Responsabile del trattamento dei dati personali é responsabile della custodia e della conservazione dei supporti utilizzati per la copia dei dati.

Per ogni banca di dati deve essere individuato il luogo di conservazione di copie dei dati, in modo che sia convenientemente protetto dai potenziali rischi di Agenti chimici, Fonti di calore, Campi magnetici, Intrusioni e Atti vandalici, Incendio, Allagamento, Furto.

Nel modulo deve essere specificato il luogo di conservazione dei supporti utilizzati per le copie dei dati.

L'accesso ai supporti utilizzati per le copie dei dati è limitato - per ogni banca di dati - a:

- Incaricati delle copie di sicurezza delle banche dati;
- Responsabile del trattamento dei dati personali.

Se il Responsabile del trattamento dei dati personali decide che i supporti magnetici contenenti dati sensibili o giudiziari non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili ed in alcun modo ricostruibili la informazioni in esso contenute.

E' compito del Responsabile del trattamento dei dati personali assicurarsi che in nessun caso vengano lasciate copie di Banche di dati contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

G. Ripristino dell'accesso ai dati in caso di danneggiamento

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento, è compito esclusivo del Responsabile del trattamento dei dati personali.

La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente ed in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro sette giorni.

Un a volta valutata l'assoluta necessità di ripristinare la disponibilità in seguito alla distruzione od al danneggiamento, il Responsabile del trattamento dei dati personali deve provvedere tramite l'Incaricato della sicurezza delle copie delle banche dati e tramite il Responsabile della gestione e della manutenzione degli strumenti elettronici all'operazione di ripristino dei dati.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo del Responsabile del trattamento dei dati personali che si può avvalere del parere del Responsabile della gestione e della manutenzione degli strumenti elettronici.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti deve essere presa rapidamente ed in ogni caso la funzionalità deve essere ripristinata al massimo entro 7 (sette) giorni.

Qualora i documenti contengano dati sensibili o giudiziari ai sensi dell'art. 4 del CODICE, gli Incaricati del trattamento sono tenuti a conservarli fino alla restituzione i contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti in cui sono presenti dati sensibili o giudiziari, è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

H. Copia degli atti e dei documenti.

In base a quanto stabilito dal CODICE e dal DISCIPLINARE, è fatto divieto a chiunque di:

- effettuare copie fotostatiche, o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- sottrarre, cancellare, distruggere, senza l'autorizzazione del Responsabile del trattamento dei dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;

- consegnare a persone non autorizzate dal Responsabile del trattamento dei dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

PARTE QUINTA

MISURE DA ADOTTARE PER LA PROTEZIONE DELLE AREE E DEI LOCALI RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITA'

Al Responsabile del trattamento spetta il compito di nominare per ciascun ufficio della struttura del titolare in cui vengono trattati i dati, un incaricato con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il Responsabile del trattamento dei dati personali deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il Responsabile del trattamenti dei dati personali deve informare con una comunicazione scritta l'incaricato dell'ufficio dei compiti che gli sono stati affidati utilizzando il modello.

PARTE SESTA

FORMAZIONE DEGLI INCARICATI DEL TRATTAMENTO

Ai sensi della regola 19.6 dell'Allegato B al CODICE, si deve procedere ad una pianificazione degli interventi formativi destinati agli incaricati del trattamento.

Il Responsabile del trattamento dei dati personali valuta, per ogni incaricato a cui ha affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.

I riscontri di tali valutazioni e le azioni adottate sono riportate nell'allegato.

La previsione di interventi formativi degli incaricati del trattamento, ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmate già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali.

Al Responsabile del trattamento dei dati personali è affidato il compito di verificare ogni anno, entro il 31 dicembre, la necessità di ulteriore informazione del personale incaricato di effettuare le copie di sicurezza delle banche di dati trattate

PARTE SETTIMA

CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DI MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

Ai sensi della regola 19.7 dell'Allegato B al CODICE, si definiscono le attività trasferite a terzi che comportano il trattamento di dati personali, identificando i responsabili del trattamento in out-sourcing, le banche dati oggetto di trattamento e le modalità di verifica di trattamento conforme anche mediante richiesta di documenti (che formano parte integrante del DPS).

I) Criteri per la scelta di enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare.

Il Titolare del trattamento dei dati personali, può affidare il trattamento dei dati, in tutto o in parte, all'esterno della struttura del titolare, a quei soggetti che abbiano i requisiti individuati all'art. 29 del CODICE (esperienza, capacità ed affidabilità).

Il Titolare cui è stato affidato il trattamento dei dati all'esterno, deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento, ai sensi del CODICE e del DISCIPLINARE.

Il Responsabile del trattamento dei dati affidati all'esterno della struttura del titolare, deve accettare la nomina secondo il modello.

II) Misure di tutela e garanzia:descrizione degli interventi effettuati da soggetti esterni.

Nel caso in cui ci si avvale di soggetti esterni alla propria struttura, per provvedere alla riparazione il Responsabile del trattamento dei dati personali, deve richiedere al tecnico che ha effettuato la riparazione, una descrizione scritta dell'intervento effettuato che ne attesti la conformità a quanto stabilito dal CODICE e dal DISCIPLINARE.

PARTE OTTAVA

PERIODICITA' DI REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Entro il 31 marzo di ogni anno, il Titolare del trattamento dei dati sensibili o di dati giudiziari deve verificare ed eventualmente predisporre una nuova versione del Documento programmatico sulla sicurezza.