

FUTURA FITNESS SAS di Farina Lorella, Merolli Marco &C.
Via Piacenza 1, 27058 Voghera (PV) C.F. e P.IVA 02377720186
Tel/Fax 0383 62813

***DOCUMENTO
PROGRAMMATICO SULLA
SICUREZZA***

(Legge 196/03 e leggi correlate)

Luogo Voghera

Data Anno 2010

Il Titolare del Trattamento dei Dati

Indice

- 1) INDICE**
- 2) PREMESSA PRINCIPALI RIFERIMENTI LEGISLATIVI**
- 3) CONSIDERAZIONI GENERALI E ATTIVITA' DELL'IMPRESA**
- 4) DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**
- 5) CUSTODIA COPIE DI SICUREZZA**
- 6) DISMISSIONE SUPPORTI RIMOVIBILI**
- 7) CIFRATURA E SEPARAZIONE DI DATI SANITARI**
- 8) ALTRE MISURE MINIME PER TRATTAMENTI CON STRUMENTI
ELETTRONICI**
- 9) NOTIFICAZIONE AL GARANTE**
- 10) CONTROLLI E SANZIONI**

Note di interesse

In riferimento agli articoli 14,15, 17 e 19 dell'allegato B del Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, la Futura Fitness A.S.D. nella persona del responsabile della sicurezza Sig. Marco Merolli, ha reso edotto i consiglieri di quanto indicato dalla delibera n° 53 del 23 Novembre 2006 " Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati".

Analogamente per il comunicato stampa del 05/03/07 del Garante per la protezione dei dati personali, in merito alle tematiche legate all'utilizzo di Internet all'interno dell'impresa.

Essendo una associazione sportiva vi è ragione di puntualizzare quanto segue:

- *I soci partecipano esclusivamente ad attività sportive e non sono direttamente interessati ad alcuna attività amministrativa, di conseguenza non hanno attinenza con la presente normativa*
- *I soci collaboratori, (istruttori) non hanno accesso ad alcuna documentazione dell'associazione, ne al database aziendale.*

Nel corso del 2007 e fino a Marzo 2008 sono state monitorate le comunicazioni del Garante per la Privacy. Non si sono avute nuove indicazioni che possano risultare congruenti con l'attività della Palestra Futura Fitness.

Si è inoltre presa visione della "Guida pratica e misure di semplificazione per le piccole e medie imprese - 24 maggio 2007 (G.U. 21 giugno 2007 n. 142). che mira a chiarire gli adempimenti a cui sono sottoposte le PMI.

In particolare ai punti:

4.1 della guida... Con particolare riferimento ai trattamenti di dati personali (non sensibili) nell'ordinaria attività d'impresa, non è necessario il consenso nei casi in cui (cfr. art. 24 del Codice):

- i dati vengono trattati nell'esecuzione di un contratto o in fase pre-contrattuale (art. 24, comma 1, lett. b), del Codice);
- il trattamento viene posto in essere per dare esecuzione a un obbligo legale (art. 24, comma 1, lett. a) del Codice);
- i dati provengono da registri ed elenchi pubblici (art. 24, comma 1, lett. c), del Codice);
- i dati sono relativi allo svolgimento di attività economiche da parte dell'interessato (art. 24, comma 1, lett. d), del Codice)

Da cui deriva che una volta resa nota la informativa sulla privacy della Futura Fitness, non è necessario ottenere il consenso per l'ordinaria attività dell'impresa.

In relazione al provvedimento di semplificazione del 27/11/08 emesso dal Garante si consente di dettare le misure minime di sicurezza anche oralmente

Si sono consultati tutti i provvedimenti del Garante della Privacy fino al Settembre 2010 e non vi sono provvedimenti che possano riguardare l'attività tipica della Futura Fitness.

Dopo aver informato il personale delle semplificazioni di cui sopra e aggiornati tutti i documenti relativi alla privacy è stata emessa la quinta edizione del DPS aggiornato in ogni sua parte, a ragione del cambio di ragione sociale della società. I cambiamenti riguardano solo l'aspetto giuridico e non già l'oggetto della medesima.

Sig. Marco Merolli

2 PREMESSA E RIFERIMENTI LEGISLATIVI

Nel corso della verifica dello stato di adeguamento alla vigente normativa in materia di protezione dei dati personali, il Titolare ha tenuto conto della seguente normativa:

- Legge 31 dicembre 1996, n. 675 “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”.
- Decreto legislativo 28 luglio 1997, n. 255 “Disposizioni integrative e correttive della L. 31 dicembre 1996, n. 675, in materia di notificazione dei trattamenti di dati personali, a norma dell’art.1, comma 1, lettera f), L 31 dicembre 1996, n. 676.
- Decreto Legislativo 13 maggio 1998, n. 171 “Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica”.
- Decreto legislativo 26 febbraio 1999, n. 51 “Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675, concernenti il personale dell’Ufficio del Garante per la protezione dei dati personali”.
- DPR 28 luglio 1999, n. 318 “Regolamento recante norme per l’individuazione delle misure minime di sicurezza nel trattamento dei dati personali previste dall’articolo 15 della legge 31 dicembre 1996, n. 675”.
- Legge 3 novembre 2000, n. 325 “Disposizioni inerenti all’adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall’articolo 15 della legge 31 dicembre 1996, n. 675”.
- Decreto legislativo 28 dicembre 2001, n. 246 “Disposizioni in materia di protezione dei dati personali, in attuazione della legge 24 marzo 2001, n. 127.
- Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”.

In sintesi, quindi, quanto richiesto dalla legge è una misura minima o una misura più adeguata e la relativa documentazione.

In termini riassuntivi, in funzione della tipologia di dati trattati (v. definizione più oltre riportata ex art. 4), occorre far fronte agli adempimenti di legge di seguito indicati:

Dati sensibili: quanto previsto dal DPS (All.B) paragrafi 3,4,5 del presente documento (oltre a quanto indicato per i dati personali)

Dati personali: paragrafo 8

Dati trattati senza l’ausilio di strumenti elettronici (personali e sensibili) : paragrafo 7

Dati sanitari (v. paragrafo 6)

3 CONSIDERAZIONI GENERALI E ATTIVITA’ DELL’IMPRESA

1. La creazione del **Documento Programmatico** è sancita nell’**art. 34 punto g) del Codice di Sicurezza** DL 30/6/2003 n. 196 e le specifiche relative al suo contenuto sono indicate in diversi punti dell’allegato B del Codice stesso (Disciplinare Tecnico in materia di misure minime di Sicurezza – artt. da 33 a 36 del Codice). E’ specificamente richiesto (All. B – 19) per i **dati sensibili** e giudiziari.
2. **La relazione accompagnatoria** del Codice in oggetto ne prevede **aggiornamenti periodici** con decreti congiunti del Ministero della Giustizia e del Ministero della Innovazione Tecnologica (art. 36) che, di conseguenza, dovranno essere seguiti con attenzione nel tempo.

Di qui anche la richiesta della **compilazione di una versione aggiornata annua entro il 31/3** (punto 19 – All. B).

3. In modo più completo, nella **Relazione accompagnatoria alla legge** stessa si legge specificamente che "Oltre alle altre definizioni sono dati personali anche quelli relativi all'uso di servizi di comunicazione elettronica" e si evidenzia quanto segue.
 - Distinzione fra elaboratori non accessibili e elaboratori in rete (disponibile o non disponibile al pubblico)
 - Obbligo di fare copie delle password
 - Obbligo autenticazione IT
 - Aggiornamento periodico compiti incaricati
 - Obbligo protezione strumenti elettronici e dati rispetto a trattamenti illeciti e accessi non consentiti
 - Aggiornamento DPSS
 - Cifratura dati salute e sessuali
 - Documento a data certa per impedimenti alle misure minime di sicurezza
 - Scadenze semestrali per sw anti intrusione (all. B 16), annuali per autorizzazioni, lista incaricati (anche per classi omogenee di incarico e profili relativi – all. B 15), aggiornamento programmi
 - Salvataggio dei dati almeno settimanale (all. B 18)
4. Il Codice di Sicurezza D.Lgs 30/6/2003 n. 196 è **entrato in vigore il 1/1/2004**.
5. In particolare il Codice si applica (art. 4) ai seguenti **soggetti**:
 - persone fisiche
 - giuridiche
 - Pubblica Amministrazione (centrale e locale)
 - "qualsiasi altro ente od organismo cui competono le decisioni in ordine al trattamento di dati personali, ivi compreso il profilo della sicurezza".
6. I dati di riferimento del Codice di Sicurezza sono:
 - dati personali
 - dati sensibili
 - dati giudiziari
7. Sono definiti come **dati personali** (art. 4): "*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*".
8. Sono definiti come **dati identificativi** (art 4): i dati che permettono l'identificazione diretta dell'interessato
9. Sono definiti come **dati sensibili** (art. 4):" "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.
10. Sono definiti come **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 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 articoli 60 e 61 del codice di procedura penale.

11. In particolare i **dati personali** possono essere oggetto di trattamenti sia all'interno del soggetto che inseriti in comunicazioni attraverso la posta elettronica.
12. Gli art 7, 10 e segg. definiscono i **diritti dell'interessato**, il **diritto al riscontro** e quando deve essere richiesto il **consenso al trattamento dei dati personali**.
13. **Più specificamente** (art. 37- a - d - e - f) **si definiscono dati personali** (per i quali occorre notificarne il trattamento al Garante)(entro il 30/4/04 – art. 181 c) “dati che:
 - indicano la *posizione geografica di persone o oggetti*
 - dati volti a definire ...o ad analizzare *le scelte dell'interessato* (ad es. tutte le sue scelte di acquisto, le sue risposte a test e/o offerte inviate, i mezzi di risposta utilizzati, le opzioni commerciali selezionate, ecc.)
 - dati necessari ai fini della *selezione del personale*
 - dati registrati in apposite banche e relativi al rischio sulla *solvibilità economica, relativi alla situazione patrimoniale e/o al corretto adempimento di obbligazioni commerciali* (quindi la maggior parte delle informazioni relative alla gestione del credito)
14. Inoltre l'art. 126 Titolo X: “**Comunicazione elettronica**”, definisce personali i dati relativi all'ubicazione dell'apparato terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.
15. Gli art. 130 e 140 forniscono regole di comportamento per le comunicazioni pubblicitarie e promozionali e per il marketing diretto (via Internet).
16. Gli art. 11, 114 e 134 definiscono i principi ai quali attenersi per la video sorveglianza dei lavoratori.
17. In particolare per i **minori** (art. 50 del Codice “notizie ...idonee ad identificare un minore”) si applicano le limitazioni previste dal DPR 448 del 22/9/88.
18. Le indicazioni in tema di definizione di **argomenti** da inserire direttamente nel **Documento Programmatico sulla Sicurezza** sono definite al punto 19 All. B, così come la periodicità degli aggiornamenti e le altre misure minime per trattamenti elettronici (art. 34 Codice e punti diversi in All. B).

Altri adempimenti di legge, sempre in termini di documentazione, sono previsti ai punti 1-18 e 25 dello stesso Allegato B.

1. Il **contenuto del Documento Programmatico** suddetto dovrà soprattutto essere descrittivo delle misure adottate rinviando ad allegati specifici i dettagli tecnici relativi alle diverse misure di sicurezza attivate.
2. Si dovranno ancora tenere presenti le principali differenze, in termini di compiti e di responsabilità delle **figure professionali aziendali coinvolte (titolare, responsabile della sicurezza, incaricati del trattamento dei dati)**, rispetto al disposto del precedente DPR 318/99 (art. 4 e segg. del Codice di Sicurezza).

A questo scopo vedasi la definizione delle stesse e l'obbligatorietà o meno della loro nomina (agli artt.4 e segg. del Codice di Sicurezza DL 30/6/2003 n. 196).

3. Infine si dovrà tenere presente, dopo la prima stesura, la creazione di ***una nuova versione del Documento Programmatico entro il 31 marzo di ogni anno*** ed in particolare si deve fare riferimento all'avvenuto aggiornamento nella ***nota accompagnatoria di bilancio*** da parte "del titolare anche attraverso il responsabile" (punti 19 e 26 all. B).
4. Per quanto attiene al trattamento di dati sensibili, giudiziari e sanitari si deve fare riferimento agli articoli 51 e segg. .

Attività dell'impresa

Palestra per attività fisiche

Note di interesse generale

Il trattamento di dati sensibili (certificati di sana e robusta costituzione, altri certificati medici, ricette di specialisti medici) sono trattati solo in forma cartacea.

4 DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Identificazione delle risorse da proteggere

4.1 Luoghi fisici.

La fase preliminare nell'individuazione del grado di sicurezza nel trattamento del dato consiste nel determinare i luoghi in cui il dato stesso viene trattato.

Sono stati analizzati i luoghi dove fisicamente si svolge il trattamento dei dati o si trovano i sistemi di elaborazione o i luoghi ove si conservano i dati. Qui di seguito si descrive, in sintesi, l'ambiente aziendale:

- i dati sono trattati in una zona aperta al pubblico all'interno della palestra, in una zona ricavata dotata di scrivania e cassetti metallici.

4.2 Ricezione pubblico.

E' quella parte della sede del Titolare aperta al pubblico, e cioè a quelle persone (clienti, fornitori, consulenti, collaboratori, etc.) interessate, per varie ragioni, all'attività del Titolare: è il luogo dove entrano ed escono i documenti (su supporto cartaceo e/o elettronico) e, quindi, i dati. E' quindi il luogo che, in assoluto, sembrerebbe evidenziare un potenziale e alto rischio di violazione della privacy e della sicurezza informatica, in quanto tale area è esposta al pubblico in genere ed agli interessati, i quali forniscono e ricevono i dati. In questa fase il rischio di interscambio di informazioni con i terzi, che non siano gli interessati, è elevato.

Di seguito la descrizione del luogo.

Vedi sopra, il luogo però è sempre presidiato dal personale e i dati sensibili sono conservati in un cassetto chiuso a chiave.

4.3 Ufficio operativo per l'elaborazione dei dati.

È l'unico angolo operativo dotato di scrivania.

4.4 Centro Elaborazione Dati (C.E.D.).(Non Applicabile)

4.5 Archivio cartaceo.

E' il luogo dove si archiviano i dati contenuti su supporto cartaceo. E' vietato l'accesso in tale luogo ai soggetti non incaricati. In questo ambiente esistono degli archivi che vengono chiusi a chiave e nei quali sono contenuti i documenti ed i dati di uso non corrente. L'accesso è meno frequente, in quanto le occasioni di necessità del dato sono ridotte rispetto all'accesso al C.E.D.

Descrivere il luogo o semplicemente il relativo armadio:

- i dati generici (schede allenamento clienti) sono affidati al singolo socio e da esso stesso conservati
- i dati amministrativi sono conservati in un armadio dotato di serratura
- i dati sensibili sono conservati in un armadio dotato di serratura

DATI SENSIBILI DI CUI AL 4.11 IN DETTAGLIO

I dati sensibili (vedi certificati di sana e robusta costituzione”e “ prescrizione di medici specialisti”) sono conservati in un armadio dotato di serratura. La chiave è in dotazione unicamente al titolare e ai consiglieri.

4.6 Risorse hardware.

Sono state analizzate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento. Tra queste particolare rilievo, hanno i personal computer, da cui vengono eseguiti i programmi che elaborano i trattamenti.

Descrivere le risorse:

1 PC con collegamento a Internet

COLLEGAMENTO A INTERNET ART 2 COMMA 2 LETTERA C, D, M,

HW di collegamento	Provider	Tipo di connessione
Scheda interna del PC	Fastcon	ADSL wireless

4.7 Personal computer

Le macchine, di recente acquisizione, sono tutte censite e l’accesso alla singola risorsa avviene tramite un’autenticazione che pilota l’utente alle sole sue informazioni.

4.8 Risorse dati

Sono stati analizzati tutti gli archivi contenenti dati personali trattati dalla ditta siano essi in formato cartaceo che in formato elettronico.

Inserire le directory contenenti i dati:

Database Spypass

4.9 Database.

La banca dati presente su questo elaboratore contiene le informazioni personali di clienti , l’accesso, avviene sempre mediante autenticazione .

4.10 Risorse software.

Sono stati analizzati i software applicativi mediante i quali vengono effettuati i trattamenti automatizzati al fine di verificare la loro corrispondenza ai requisiti minimi.

	Nome	Produttore	Descrizione	Postazione
01	Windows Vista	Microsoft	SW Operativo	Unica
02	Windows Sette	Microsoft	SW Operativo	Unica

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Si suggerisce di specificare quanto sopra attraverso le seguenti informazioni:

- nome interno (aziendale) dell'applicazione (in chiaro ed eventualmente in codice)
- breve descrizione della stessa con note sulla periodicità di effettuazione e sulle principali funzionalità previste e utilizzate
- rinvio ad allegati di documentazione (se esistenti) per maggiori dettagli sia funzionali che tecnici
- riferimento alla notifica al Garante richiesta dal Codice (art. 37)
- copia della modulistica utilizzata

E', infine, da ricordare che :

- la durata del trattamento dei dati deve protrarsi "fino al perseguimento delle finalità del trattamento stesso"
- per alcuni trattamenti (ad es. quelli relativi a dati sensibili – come definiti all'art.4)– occorre il consenso scritto dell'interessato
- che vige l'obbligo della trasparenza ad es. verso i dipendenti per il trattamento di dati che li interessano direttamente

SITO INTERNET

Il sito è all'indirizzo www.futurafitness.com .

Laddove siano pubblicate foto di soci, viene chiesta apposita liberatoria nella richiesta di ammissione a socio.

4.11 Schede rilevazione risorse dati

DATI SOFTWARE

Supporto utilizzato	Nome Directory	Hardware supporto	di	Descrizione dati contenuti	Tipologia di dati
Database	Sypass	PC Unico		Dati anagrafici clienti Dati identificativi Abbonamento sottoscritto Vari	Personali

DATI CARTACEI

Tipo di documento	Dislocazione fisica	Tipologia di dati
Schede allenamento	Presso soci	Personali
Fatture fornitori	Armadio con serratura nella reception	Personali
Ricevute fiscali clienti	Armadio con serratura nella reception	Personali
Fatture clienti	Armadio con serratura nella	Personali

	reception	
Certificati medici di sana e robusta costituzione	Armadio con serratura nella reception	Sensibili
Prescrizioni terapeutiche di medici specialisti	Armadio con serratura nella reception	Sensibili

4.12 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (all. B-19.2)

- Individuazione del titolare del trattamento

Merolli Marco

- Anagrafica dell'impresa titolare del trattamento
FUTURA FITNESS SaS di Farina Lorella, Merolli Marco & C.
Via Piacenza s.n. 27058 Voghera (PV) C.F. e P.IVA 02377720186
Tel/Fax 0383 62813

Il CDA ha nominato "Titolare del trattamento" il Sig. Merolli Marco (vedi lettera di nomina allegata)

Egli avrà i seguenti compiti operativi

- garantire la sicurezza dei dati aziendali , in particolare ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito

Per far ciò il CDA ha nominato "Responsabile del trattamento dei dati " il Sig. Merolli Marco. (vedi lettera di nomina allegata)

Egli avrà i seguenti compiti operativi

- impedire con ogni mezzo tecnicamente ed economicamente praticabile i rischi connessi al trattamento dei dati
- assegnare le User ID agli user e le relative Password
- cancellare le medesime in caso di dismissione dell'incarico
- custodire le medesime in luogo protetto
- attivare tutte le misure di salvataggio periodico dei dati
- Attivare i sistemi di antintrusione elettronica
- Gestire nel tempo i sistemi sopraccitati
- Aggiornare il DPS
- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco delle tipologie dei trattamenti effettuati
- Distruggere i dati laddove non vi sia più la necessità di utilizzazione
- Attribuire i compiti ai titolari di trattamento dei dati
- Informare il titolare nel caso i cui si siano rilevati dei rischi
- Favorire la loro formazione in termini di sicurezza e trattamento dei dati

La nomina è a tempo indeterminato, salvo revoca da parte del titolare del trattamento o dimissioni da parte del responsabile.

4.13 Analisi dei rischi che incombono sui dati (all. B-19.3)

I rischi che incombono sui dati in esame sono sostanzialmente dipendenti da fattori quali:

- l'entità dei dati gestiti

- la frequenza di trattamento
- le tecniche di salvataggio periodico dei dati
- le tecnologie informatiche presenti in azienda
- il numero di utenti (interni ed esterni) che accedono a tali dati
- le modalità di aggiornamento delle Basi Dati che li contengono

Sulla scorta di quanto sopra, indichiamo:

- il rischio sia in termini descrittivi che di valore (o stima) dello stesso e di probabilità di accadimento
- le misure adottate al fine di ridurlo per la perdita (totale o parziale) dei dati trattati
- il rinvio ad eventuali documenti tecnici che descrivano in dettaglio le misure stesse
- il rischio residuo che permane per ogni trattamento degli stessi dati
- il valore di tale rischio

ANALISI DEI RISCHI SUI LUOGHI FISICI

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Tutte	Possibilità di intrusione	Media	Porte e finestre con vetri antisfondamento.
Tutte	Allagamenti	Bassa	Area non soggetta ad esondazioni o calamità di questo tipo
Tutte	Incendio	Bassa	Non vengono usate fiamme libere. Impianto elettrico soggetto ad interruttore inerziale.
Tutte	Furto	Media	Porte e finestre con vetri antisfondamento.
Tutte	Impossibilità di rilevare accessi non autorizzati	Bassa	La palestra ha un solo accesso sempre presidiato durante il normale svolgimento dell'attività lavorativa

ANALISI DEI RISCHI SULLE RISORSE HARDWARE

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Tutte	Uso non autorizzato dell'hardware	Bassa	L'utilizzo dell'hardware è soggetto all'utilizzo di password
Tutte	Manomissione/sabotaggio	Bassa	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia.
Tutte	Probabilità/frequenza di guasto	Bassa	L'hardware acquistato è di qualità e storicamente non ha mai dato problemi rilevanti.
Tutte	Intercettazione delle trasmissioni	Media	Il modem è collegato direttamente alla rete telefonica pubblica.

Tutte	Rischi connessi all'elettricità.	Bassa	An xatech tech 650 lcd gruppo di continuità
-------	----------------------------------	-------	---

ANALISI DEI RISCHI SULLE RISORSE DATI

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Tutte	Accesso non autorizzato	Bassa	L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti da password. All'archivio cartaceo (sensibili) possono accedere solo i diretti incaricati che possiedono la chiave dell'armadio.
Tutte	Cancellazione non autorizzata di dati/manomissione di dati	Bassa	L'accesso agli elaboratori avviene solo tramite gli elaboratori protetti da password. All'archivio cartaceo (sensibili) possono accedere solo i diretti incaricati che possiedono la chiave dell'armadio.
Tutte	Perdita di dati	Bassa	I dati sono conservati su chiave USB. Sono effettuate copie settimanali di backup.

ANALISI DEI RISCHI SULLE RISORSE SOFTWARE

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
Tutte	Accesso non autorizzato alle basi dati connesse	Bassa	I software che trattano i dati controllano l'accesso tramite una finestra di autenticazione (finestra di Login).
Tutte	Errori software che minacciano l'integrità dei dati	Bassa	I software sono utilizzati da parecchi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati
Tutte	Presenza di codice non conforme alle specifiche del programma	Bassa	I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni.

4.14 Misure per l'integrità e la disponibilità dei dati (all. B-19.4.1)

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, si definiscono:

- gli strumenti hardware utilizzati per il salvataggio (back -up)
- l'eventuale riutilizzo sistematico
- i responsabili del salvataggio

- le frequenze di salvataggio
- le modalità di conservazione delle copie

Il salvataggio deve avvenire almeno una volta al mese.

STRUMENTI E POLITICHE DI SALVATAGGIO

Dispositivo di backup:	<input type="checkbox"/> Non esistente <input checked="" type="checkbox"/> Sì, presente Tipo/Modello : chiave USB Frequenza di backup: mensile
Incaricati del backup:	1) Merolli Marco
Supporti di backup:	Numero di supporti: 1 chiave USB Luogo di conservazione: La chiave viene rimossa ogni sera e portata con se dal titolare
Procedura di Back up	La procedura manuale deve essere attivata a cura dell'incaricato .
Directory o database soggetti a back up.	Il database Spypass
Durata della conservazione	Infinita fino a obsolescenza dei dati e relativa distruzione

4.15 Criteri e modalità di ripristino della disponibilità dei dati in caso di distruzione o danneggiamento (all. B-19.5)

Il Responsabile di sistema è responsabile della custodia e della conservazione di supporti utilizzati per il back-up dei dati.

Per ogni banca dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up dei dati.

L'accesso ai supporti utilizzati per il back-up dei dati è limitato per ogni banca di dati a:

- Titolare e Responsabile della sicurezza dei dati

E' compito del Responsabile di sistema assicurarsi che in nessun caso vengano lasciate copie di back-up delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

Premesso quanto sopra, in termini di documentazione si tratta quindi di descrivere, sempre in modo esauriente e facilmente comprensibile, tutte le procedure attivate per il ripristino dei dati in caso di loro danneggiamento o distruzione.

STRUMENTI E POLITICHE DI RIPRISTINO

Incaricati del ripristino:	Merolli Marco
Procedura di Ripristino	La procedura è manuale e deve essere attivata a cura dell'incaricato presente. È necessario Inserire/collegare lo strumento di ripristino e avviare la procedura inversa a quella di back up.

	Al termine è necessario aprire almeno un documento per ogni directory e per ogni tipologia in modo da assicurarsi dell'integrità dei medesimi. È buona cosa procedere inoltre alla modifica dei documenti ad esempio inserendo una lettera alfabetica e risalvare il documento, provare inoltre se il documento è stampabile.
--	--

4.16 Protezione delle aree e dei locali (all. B-19.4.2)

Vedere paragrafo 4.4 al punto “analisi dei rischi sulle risorse dati”.

Indicare di seguito eventuali persone terze che potrebbero accedere ai dati e le misure prese per limitare il rischio.

Vedi al 4.13.

4.17 Previsione di interventi formativi degli incaricati del trattamento (all. B-19.6)

Al responsabile della sicurezza dei dati è affidato il compito di verificare ogni anno, le necessità di formazione del personale incaricato.

Per ogni incaricato del trattamento il responsabile della sicurezza dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata, comunicando in forma scritta ai collaboratori le necessità formative e documentando la formazione eseguita.

Si tratta quindi di approntare un modulo per la descrizione degli interventi formativi praticati, i collaboratori che hanno partecipato al corso la data e la durata del medesimo.

In particolare si renderà necessaria opera di formazione allorquando:

- introduzione di nuove tecnologie hardware
- cambio della logistica dei locali
- passaggio di un operatore da una funzione ad un'altra
- introduzione di nuovi software
- assunzione di personale.

N.B. in relazione alla semplificazione adottata dal garante “Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008

G.U. n. 287 del 9 dicembre 2008, è possibile impartire istruzioni anche oralmente.

Criteria per le misure minime di sicurezza in caso di trattamenti esterni di dati personali (all. B-19.7)

Il trattamento esterno dei dati è affidato per quanto attiene alle pratiche amministrative/contabili/fiscali/retributive allo studio **Dott. Castronovo Salvatore, Voghera (PV)**. Esso si preoccupa di trattare i dati secondo la normativa vigente D.L. 196/03 e leggi correlate. Ulteriori trattamenti esterni sono quelli relativi alle contabili bancarie e quindi alle banche di cui l'azienda è cliente che sono:

Banca Intesa Agenzia di Voghera Via Plana 42 o alla sua succursale di C.so 27 Marzo.

Nessun altro utilizzo è previsto o autorizzato.

5 CUSTODIA DI COPIE DI SICUREZZA (All. B-21 e 27)

Il luogo di conservazione deve essere individuato in modo che sia protetto da:

- agenti chimici
- fonti di calore
- campi magnetici
- intrusioni ed atti vandalici
- incendio
- allagamento
- furto

In particolare per ogni banca di dati sono 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 e 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
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le copie di back-up
- Le istruzioni ed i comandi necessari per effettuare le copie di back-up.

Luogo di conservazione dei supporti di back up	La chiave di back up viene conservata personalmente dal responsabile della sicurezza e portata con se dopo la chiusura.
---	---

6 DISMISSIONE SUPPORTI RIMOVIBILI (All. B-22)

Se il Responsabile di sistema decide che i supporti magnetici utilizzati per le copie di back-up delle banche di dati trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a cancellare il contenuto annullando e rendendo illeggibili le informazioni in esso contenute.

E' compito del Responsabile di sistema assicurarsi che in nessun caso vengano lasciate copie di back-up delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

Il Responsabile darà evidenza degli supporti informatici o cartacei distrutti o delle directory o database eliminati con la scheda di seguito indicata che farà riferimento alle eliminazioni eseguite nell'anno precedente alla stesura e aggiornamento del presente DPS.

Tipo di supporto	Tipo di archivio o di documenti	Metodo di eliminazione	Autore eliminazione	Data eliminazione
Chiave	Anagrafica	Rottura supporto	Responsabile	

Anche nel caso di dismissione di supporti informatici (PC) il disco è soggetto a formattazione di basso livello e successiva rottura.

Il supporto informatico è dato per lo smaltimento a ditte autorizzate allo smaltimento.

Tipo di supporto	Tipo di archivio o di documenti	Metodo di eliminazione	Autore eliminazione	Data eliminazione
Dischi rigidi estribili	Tutti	Cancellazione e rottura meccanica del dispositivo	Responsabili back up	Varia

*come da provvedimento del garante emesso in data 13/10/08 art 1.

7 CIFRATURA E SEPARAZIONE DI DATI SANITARI (art. 24 e All. B-19.8)

In considerazione della natura particolare dei dati interessati alla norme di legge (si parla specificamente di dati idonei a rivelare lo stato di salute e la vita sessuale e di organismi sanitari e di organismi esercenti le professioni sanitarie), dovranno essere adottate misure supplementari di seguito indicate.

I dati sanitari che sono:

- Certificati medici di sana e robusta costituzione
- Prescrizioni terapeutiche di medici specialisti

Sono esclusivamente cartacei (non vengono archiviati informaticamente) e vengono conservati in un armadio presso la reception dotato di serratura.

Detto ufficio è dotato di serratura a chiave in dotazione solo agli incaricati.

L'accesso ai dati è consentito agli incaricati (vedere lettera di nomina).

8 ALTRE MISURE MINIME PER TRATTAMENTI CON STRUMENTI ELETTRONICI

Come già accennato l'art. 34 del Codice l'All. B prevedono una serie di misure minime che dovranno essere adottate e documentate dalle aziende per i trattamenti dei dati personali.

Vediamole in dettaglio.

8.1 Sistema di autenticazione delle informazioni (all. B-1-11)

Per l'accesso ai dati gli incaricati dispongono di un codice di identificazione "User ID" associato ad una parola chiave".

L'elenco degli utilizzatori e delle relative parole chiave è conservato dal Responsabile del sistema in busta chiusa.

Laddove uno o più incaricati siano autorizzati ad accessi limitati nel modulo che evidenzia e raccoglie queste informazioni vi è l'indicazione anche agli archivi consentiti a ciascun incaricato.

Le parole chiave devono essere di almeno 8 caratteri o inferiore laddove il sistema operativo non consenta questa possibilità.

Si richiede inoltre, sempre per le parole chiave, che le stesse non contengano riferimento facilmente riconducibili all'incaricato e siano modificabili dall'incaricato al primo utilizzo e successivamente almeno ogni 6 mesi (punto 5) **(rimane ogni 6 mesi in quanto i dati sensibili sono trattati solo in forma cartacea)**

Le parole chiave o il dispositivo di sicurezza assegnato non possono essere trasferite ad altri incaricati (punto 6)

Le credenziali non utilizzate da 6 mesi devono essere disattivate, salvo quelle utilizzate per soli scopi di gestione tecnica (punto 7)

In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati si dovrà provvedere a disattivare immediatamente la possibilità di accesso al sistema per il soggetto in questione.

8.2 Descrizione del sw anti intrusione (All. B 16)

utilizzato per evitare il danneggiamento dei dati personali (All. B - punto 16)

- descrizione del tipo di sw utilizzato e delle modalità di installazione attivate
- documentazione del suo aggiornamento **(che si richiede almeno semestrale)**

Il programma di anti virus deve essere lanciato con frequenza almeno settimanale.

Nel caso in cui il sistema rilevi un virus che non sia possibile isolare e mettere in quarantena automaticamente ma che richieda una procedura più complessa è necessario chiedere l'assistenza tecnica del fornitore del programma stesso.

Il Programma Antivirus ha una scansione giornaliera alle ore 22.00.

SOFTWARE ANTI INTRUSIONE	
Modello	Firewall di Windows Vista
Casa Produttrice	Microsoft
PC protetti	Unico
Installazione sw	Autoinstallato

SOFTWARE ANTI VIRUS	
Modello	Trend Micro Internet security
Casa Produttrice	Trend Micro Corporation
PC protetti	Unico
Installazione sw	Autoinstallato
Modalità di lancio	Scansione in tempo reale

8.3 Documentazione degli aggiornamenti dei programmi (All. B 17)

“volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti”
(All. B-punto 17)

- **aggiornamento del punto precedente almeno annuale**

Al Responsabile di sistema è affidato il compito di verificare ogni anno, la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità del software applicativo, 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 della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

AGGIORNAMENTO PROGRAMMI

Programma aggiornato	Eseguita da	Frequenza aggiornamento
Windows Vista	Microsoft	Automatica ad ogni collegamento alla rete internet.
SpyPass	GSZ	Con frequenza stabilita dal produttore (il database è semplicemente una anagrafica dei clienti e scadenziario pagamenti, per cui l'aggiornamento è di fatto inutile non avendo risvolti fiscali).

8.4 Dichiarazione scritta della conformità degli interventi esterni (All. B – punto 25)

Risorse esterne alla struttura che operano sui mezzi elettronici del soggetto, devono descrivere l'intervento effettuato e attestarne l'esecuzione in conformità a tutte le disposizioni dell'All. B.

- descrizione degli interventi effettuati da personale esterno (installazioni di hw e sw, servizi di consulenza, ecc.) che attestino la conformità al disposto dell'All. B del Codice di Sicurezza (Disciplinare Tecnico)

9 NOTIFICAZIONE AL GARANTE

La legge prevede, infine, (art. 37) la notificazione al Garante di alcuni dati personali (come indicato dall'articolo stesso), la cui notificazione sarà inserita in un pubblico registro consultabile elettronicamente.

Tale comunicazione deve avvenire solo nei casi indicati dall'art. 37

Le modalità di notificazione sono precisate nell'art. 38 e segg. del Codice di Sicurezza.

In una sua newsletter del luglio 2003 il Garante (ora non più denominato Garante per la privacy bensì Garante per la protezione dei dati personali) precisa che la notificazione è dovuta da parte delle aziende che, con strumenti elettronici :

- utilizzano la profilazione dei consumatori
- usano dati per la selezione del personale
- fanno ricerche di marketing
- usano informazioni commerciali relative alla solvibilità

In particolare il Garante per la protezione dei dati personali ha inserito nel suo sito: www.garanteprivacy.it, le istruzioni ufficiali per la compilazione della notificazione e la modulistica relativa.

Sempre dallo stesso sito è possibile scaricare il software per la notificazione e la trasmissione della stessa al Garante.

10 CONTROLLI E SANZIONI

La materia è trattata in modo molto dettagliato nella Parte III del Codice: Tutela dell'interessato e sanzioni (artt. 141 e segg.).

In sintesi si prevede quanto segue:

- art. 158 – 2: il *Garante si avvale di altri organismi statali (v. convenzione 10/02 con GGFF)* per effettuare i controlli
- art. 161: qualora *non* sia stata data *comunicazione agli interessati circa la natura e l'utilizzo dei propri dati* è prevista una sanzione da 3.000 a 30.000 €
- art. 162: qualora siano stati *ceduti a terzi senza autorizzazione i dati personali* trattati è prevista una sanzione da 5.000 a 30.000 €
- art. 163: *l'omessa o incompleta notifica al Garante* (v. sopra) comporta una sanzione da 10.000 a 60.000 €. Una *falsa notifica* comporta una pena da 6 mesi a 3 anni di reclusione.
- art. 164: *l'omessa o incompleta esibizione all'autorità controllante* dei documenti richiesti prevede una sanzione da 4.000 a 24.000 €
- art. 167: il *trattamento illecito dei dati personali* prevede una reclusione da 6 mesi a 3 anni
- art. 169: *la mancata adozione delle misure minime di sicurezza* comporta una pena da 10.000 a 50.000 € ed il blocco del trattamento. L'adempimento entro 60 giorni dall'avvenuto controllo comporta la riduzione dell'ammenda ad ¼ di quella stabilita. In ogni caso il tempo massimo concesso per l'adempimento è di 6 mesi.

Oltre a quanto sopra indicato, l'articolo fa riferimento alla Legge 547/93 “ Crimini informatici commessi da dipendenti ed addebitabili all'azienda” e all'art. 2050 Cod. civile “Responsabilità oggettiva per l'esercizio di attività pericolosa” (il trattamento dei dati è giudicato tale dallo stesso articolo).

Tali norme prevedono:

- **Sanzioni a seguito di controllo ispettivo della GGFF (recente passaggio di responsabilità – v. GU 10/02) fino a 124.000 €.**

art. 170: inosservanza provvedimento Garante su *dati sensibili*(ex art. 26 comma 2): reclusione da 3 mesi a 2 anni.