Il presente documento viene redatto in aderenza alle disposizioni di cui al Decreto Legislativo 30 giugno 2003, n. 196, artt. da 33 a 36 (*misure minime di sicurezza*) nonché dal disciplinare tecnico contenuto nell'allegato B del citato decreto. In particolare:

- l'art. 34, comma 1, lettera g) del D.Lgs. 196/2003 prevede nel caso di trattamento di dati personali effettuato con strumenti elettronici l'obbligo della "tenuta di un aggiornato documento programmatico sulla sicurezza";
- il punto 19 dell'allegato B definisce le idonee informazioni necessarie per redigere il predetto documento, che di seguito viene più semplicemente definito DPS.

In particolare, sulla base delle regole previste dal disciplinare tecnico, il DPS è strutturato nelle seguenti sezioni:

sezione	**contenuto**
19.1	Elenco dei trattamenti di dati personali
19.2	Distribuzione dei compiti e delle responsabilità
19.3	Analisi dei rischi
19.4	Misure esistenti e da adottare
19.5	Criteri e modalità di ripristino della disponibilità dei dati
19.6	Pianificazione degli interventi formativi
19.7	Trattamenti affidati all'esterno

(solo per gli organismi sanitari e gli esercenti le professioni sanitarie è necessario prevedere anche la seguente ulteriore sezione)

19.8	Cifratura dei dati o separazione dei dati identificativi

---

Il presente documento viene redatto da …….. nella sua qualità di …… (*titolare/responsabile*) della sicurezza della società (*o studio o altro*) ……., che provvede e sottoscriverlo in calce.

Il DPS è inoltre corredato dalla seguente documentazione, che si riporta in allegato:

(*riportare eventualmente in allegato fac-simili e carte di lavoro predisposte, quali ad esempio l'informativa, la lettera di incarico al responsabile o agli incaricati del trattamento, l'autorizzazione al trattamento da parte dell'interessato, ecc…)*

- ……
- ……
- ……
- ……
- ……
- ……

Regola 19.1 Elenco dei trattamenti di dati personali.

La società (*o studio o altro*) …… tratta i seguenti dati personali:

(di seguito si forniscono alcuni esempi, relativi a situazioni comuni, soprattutto con riguardo ad uno studio professionale; l'elenco è ovviamente integrabile a seconda delle specifiche esigenze del soggetto obbligato)

- dati personali non sensibili dei clienti, dei fornitori o di terzi ricavati o ricavabili da elenchi pubblici, albi professionali o camerali, visure e certificati camerali;
- dati personali non sensibili dei clienti, forniti al fine di espletare gli incarichi affidati al titolare del trattamento, compresi i dati sul patrimonio o sulla situazione economica;
- dati personali non sensibili di soggetti terzi, forniti dai clienti per l'espletamento degli incarichi affidati al titolare del trattamento, o relativi alla reperibilità e alla corrispondenza con gli stessi;
- dati personali non sensibili di fornitori, affidati al titolare del trattamento al fine della reperibilità e della corrispondenza con gli stessi, nonché per fini contabili, fiscali, o di natura bancaria;
- dati personali non sensibili dei dipendenti e dei collaboratori, necessari al regolare svolgimento del rapporto di lavoro o di collaborazione, alla reperibilità e alla corrispondenza con gli stessi, o richiesti ai fini fiscali, previdenziali, nonché quelli affidati al datore di lavoro per esigenze di natura bancaria.

La società (*o studio o altro*) …… tratta i seguenti dati sensibili:

(anche in questo caso si riportano solo degli esempi, integrabili e modificabili a seconda delle specifiche esigenze del compilatore)

- dati sensibili del personale dipendente, relativi a …….., idonei a rivelare ……. (*per esempio stato di salute o vita sessuale*);
- dati sensibili dei clienti, relativi a ……..., idonei a rivelare ……. (*per esempio stato di salute o vita sessuale*).

Nella tabella 1.1 che segue si elencano schematicamente i trattamenti esistenti alla data di redazione e sottoscrizione del DPS, compresa ogni utile informazione idonea ad identificare inequivocabilmente il trattamento, la struttura aziendale all'interno della quale il trattamento viene eseguito, gli strumenti utilizzati nel trattamento. Per questi ultimi, ove necessario, sono indicati ulteriori elementi necessari alla miglior individuazione di quanto tecnicamente utilizzato a supporto del singolo trattamento.

Tabella 1.1 - Elenco dei trattamenti				
1 Identificativo		Descrizione		
Natura dei dati (1)	[ ] Personali [ ] Sensibili		[ ] Giudiziari	Data di aggiornamento
Strutture aziendali (2)			Strutture esterne (3)	
Strumenti utilizzati:				
Banca dati utilizzata	Ubicazione fisica supporti		Tipo dispositivi di accesso	Tipo di interconnessione
2 Identificativo		Descrizione		
Natura dei dati (1)	[ ] Personali [ ] Sensibili		[ ] Giudiziari	Data di aggiornamento
Strutture aziendali (2)			Strutture esterne (3)	
Strumenti utilizzati:				
Banca dati utilizzata	Ubicazione fisica supporti		Tipo dispositivi di accesso	Tipo di interconnessione

3	Identificativo		Descrizione		
Natura dei dati (1)		[ ] Personali [ ] Sensibili [ ] Giudiziari		Data di aggiornamento	
Strutture aziendali (2)			Strutture esterne (3)		
Strumenti utilizzati:					
Banca dati utilizzata		Ubicazione fisica supporti	Tipo dispositivi di accesso	Tipo di interconnessione	

Note:
(1) barrare la casella interessata
(2) va riportata l'indicazione di massima del reparto/ufficio/funzione aziendale coinvolta; questa casella è correlata all'indicazione analitica dei soggetti interessati evidenziata nella sezione che segue (19.2, tabella 2.1)
(3) riportare gli eventuali soggetti esterni alla società che operativamente effettuato il trattamento o parte di esso

---
(di seguito si propone un esempio di compilazione della tabella)

Tabella 1.1 - Elenco dei trattamenti					
1	Identificativo	**DIP/01**	Descrizione	Dati del personale dipendente	
Natura dei dati (1)		[**X**] Personali [**X**] Sensibili	[ ] Giudiziari	Data di aggiornamento	27/05/04
Strutture aziendali (2)		Divisione amministrativa area E Divisione segreteria area O	Strutture esterne (3)	Consulente del Lavoro Dott. XY	
Strumenti utilizzati:					
Banca dati utilizzata		Ubicazione fisica supporti	Tipo dispositivi di accesso	Tipo di interconnessione	
		1) Armadio chiuso a chiave nell'ufficio del personale 2) Cassaforte in segreteria (dati per legge 626)			
Foglio di lavoro \server\dipendenti.xls		Memorizzazione sul server, Stanza EDP, chiusa a chiave, non accessibile	Riservato alla divisione amministrativa (area E) e alla divisione segreteria (area O); accesso mediante password	Connessione in rete TCP/IP	

Regola 19.2 Distribuzione dei compiti e delle responsabilità.

La società (*o studio o altro*) ……. è già dotata di un organigramma e di un mansionario che di seguito viene integralmente riportato. Anche in questo documento, come in altri già utilizzati dalla società, i riferimenti ai componenti strutturali vanno fatti a questo documento:

(di seguito si propone un modello di organigramma e mansionario aziendale; lo stesso risulta peraltro discretamente analitico, e quindi ciascun utilizzatore potrà adattarlo alle proprie specifiche esigenze)

Quadro di sintesi

Divisione Amministrativa					Divisione Direzionale						Divisioni Operative	Divisione Segmento 1	Divisione Segmento 2	Divisione Segreteria		
A	B	C	D	E	F	G	H	I	J	K		L	M	N	O	P

Divisione Amministrativa

Area A: Contabilità e bilancio
- Sovrintende alla redazione della contabilità, concordando con la persona addetta metodologie e scritturazioni
- Predispone la bozza di bilancio da sottoporre al Consiglio di Amministrazione
- Sovrintende alla redazione del bilancio definitivo da sottoporre all'approvazione dei soci
- Sovrintende alla redazione delle dichiarazioni fiscali

Area B: Fatturazione e valorizzazione prestazioni.
- Sovrintende alla redazione delle fatture
- Coordina l'attività di reperimento dei dati al fine della corretta fatturazione
- Coordina l'attività di controllo interno delle prestazioni fatturate
- Pianifica e coordina i budget annuali degli importi da fatturare
- Sovrintende al controllo del fatturato rispetto agli impegni contrattuali assunti (mandati)
- Sovrintende alla gestione delle anticipazioni di cassa
- Coordina e trasmette i report periodici
- Coordina l'attività di recupero crediti

Area C: Pianificazione e controllo di gestione
- Predispone il budget preventivo dei costi
- Sovrintende al controllo di gestione
- Autorizza gli ordini di acquisto, provenienti dalle diverse aree

Area D: Gestione finanziaria
- Sovrintende alla gestione della cassa
- Sovrintende alla gestione delle anticipazioni
- Sovrintende alle operazioni eseguite tramite banca
- Cura il rapporto con gli istituti di credito
- Coordina e trasmette i report finanziari periodici

Area E: Personale
- Sovrintende alla monitorizzazione delle presenze mensili
- Cura i rapporti con il consulente del lavoro
- Coordina le ferie, i permessi, le assenze del personale
- Sovrintende alla gestione delle assenze
- Sovrintende alla consegna dei cedolini mensili, e di altri eventuali documenti

Divisione Direzionale

Area F: Formazione e Risorse Umane
- Coordina l'attività di selezione del personale
- Sovrintende alla formazione, sia interna che esterna, delle risorse umane, sia in fase di start-up che periodicamente, coordinando l'utilizzo di persone e strumenti formativi

- Coordina l'attività di valutazione periodica del personale
- Sovrintende alla gestione del registro degli infortuni professionali

Area G: Marketing
- Pianifica e sovrintende all'attività di promozione dell'immagine
- Coordina l'attività di "customer satisfaction"

Area H: Sicurezza
- Sovrintende alla corretta gestione degli adempimenti legati alla legge 626 (sicurezza sul lavoro)
- Sovrintende alla corretta gestione degli adempimenti legati al D.Lgs. 196 (privacy)

Area I: Gestione del Patrimonio
- Sovrintende alla manutenzione dei beni
- Pianifica la sostituzione degli stessi beni
- Sovrintende alla disposizione degli ambienti di lavoro
- Sovrintende alla preservazione dei beni contro furto, incendio, intrusione
- Sovrintende alla gestione degli impianti di allarme

Area J: TQM
- Coordina l'acquisizione, la produzione, la divulgazione, il corretto utilizzo delle procedure
- Sovrintende alla predisposizione dei documenti da utilizzare, previa approvazione della Direzione Generale

Area K: EDP
- Gestisce la manutenzione, l'upgrade, la sostituzione, del materiale elettronico
- Gestisce tutto il software dello studio, compresa la gestione delle licenze d'uso dei programmi
- Coordina e sovrintende al backup degli archivi elettronici
- Coordina la realizzazione, interna o esterna, di strumenti e procedure informatiche, su sollecitazione propria o delle diverse divisioni ed aree

Divisione operativa Segmento 1

Area L
- …

Divisione operativa Segmento 2

Area M
- …

Divisione operativa segreteria

Area N: Front office
- Gestisce le comunicazioni telefoniche e via fax
- Gestisce la corrispondenza in entrata e in uscita
- Gestisce la battitura dei testi
- Gestisce il servizio di circolari ricevute e di circolari ai clienti
- Gestisce la prenotazione e la preparazione della sala riunioni

Area O: Back office
- Gestisce l'archiviazione cartacea ed elettronica di tutta la documentazione

- Gestisce la biblioteca (libri e riviste in entrata, in uscita, collocazione fisica, aggiornamenti e abbonamenti)
- Gestisce gli accessi e le vacazioni presso uffici, clienti, enti, coordinandosi con l'area B - Fatturazione
- Gestisce la "piccola cassa" e la "cassa valori bollati", relazionando all'area D - Gestione finanziaria
- Gestisce lo "scadenziario"
- Gestisce le dichiarazioni dei sostituti di imposta (Mod. 770)

Area P: Manutenzione attrezzature
- Gestisce l'ordinaria manutenzione di tutte le attrezzature e macchinari, con esclusione delle macchine elettroniche di pertinenze dell'area K - EDP
- Gestisce i materiali di consumo e la cancelleria, verificando le scorte minime e proponendo gli ordini di acquisto alla divisione amministrativa

Organigramma

DIVISIONI		DIREZIONE	AREE	Responsabile	Addetti
DIVISIONI	Amministrativa		A contabilità		
			B fatturazione		
			C controllo di gestione		
			D gestione finanziaria		
			E personale		
	Direzionale		F risorse umane		
			G marketing		
			H sicurezza		
			I patrimonio		
			J TQM		
			K EDP		
	Segmento 1		L		
	Segmento 2		M		
	Segreteria		N front office		
			O back office		
			P manutenzione		

Considerando quindi le risorse a disposizione della struttura aziendale, nella tabella 2.1 sono specificatamente riportate le informazioni in materia di sicurezza del trattamento dei dati.

Tabella 2.1 – Strutture preposte ai trattamenti				
1	Struttura (1)		Data di aggiornamento	
Dati riferiti ai singoli trattamenti				
Responsabile		Trattamento operato (2)	Compiti della struttura	
2	Struttura (1)		Data di aggiornamento	
Dati riferiti ai singoli trattamenti				
Responsabile		Trattamento operato (2)	Compiti della struttura	
3	Struttura (1)		Data di aggiornamento	
Dati riferiti ai singoli trattamenti				
Responsabile		Trattamento operato (2)	Compiti della struttura	

Note:
(1) indicare la struttura aziendale, coordinando il dato con quanto già redatto nella precedente sezione in tabella 1.1
(2) indicare il trattamento, così come identificato in tabella 1.1

(di seguito si propone un esempio di compilazione della tabella)

1	Struttura (1)	Divisione amministrativa area E	Data di aggiornamento	27/05/2004
Dati riferiti ai singoli trattamenti				
Responsabile		Trattamento operato (2)	Compiti della struttura	
Mario Rossi		**DIP/01**	Intera gestione del personale come risulta dal mansionario	

Regola 19.3 Analisi dei rischi.

La totalità dei dati trattati possono essere conservati, alternativamente o contemporaneamente, in fascicoli riposti in schedari dotati di chiusura, in locali protetti, archiviati al termine della pratica, e tramite personal computer connessi in rete.

(di seguito si propone un esempio di illustrazione della sede aziendale)

Le sede della società (*o studio o altro*), ove vengono trattati i dati, è ubicato …….. (*per esempio in un condominio in zona periferica/industriale/…, o in un singolo stabile sito in ……),* dotato di portoncino blindato (*o porta scorrevole a vetri, o porta con chiusura automatica, ecc….*) e con videocitofono, con (*o senza*) sorveglianza notturna, dotato di sistema di allarme.
Le singole stanze che compongono la sede sono dotati di chiave, così come l'archivio, la stanza EDP, la biblioteca, ecc …. La segreteria è situata in un locale ampio, nell'immediato ingresso della sede, dove in zona separata e opportunamente distanziata dai posti di lavoro è stata ricavata una sala di attesa per clienti, fornitori, rappresentanti, ecc…
La stanza archivio (*o segreteria, o altro*) è dotata di cassaforte con chiusura a chiave (*o a combinazione, ecc…*)
Ogni ufficio è dotato di personal computer in rete e connesso ad Internet con connessione ADSL. In segreteria sono centralizzati i seguenti dispositivi:
- stampante laser;
- fax a carta comune;
- fotocopiatrice;
- ….

E' stata compiuta l'analisi dei rischi, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonché all'impatto sulla sicurezza dei dati, in relazione a ciascun evento e alla gravità e probabilità stimata dell'evento steso. Per ciascun eventi probabile, si è ipotizzato naturalmente la contromisura adottata o da adottare.

Sinteticamente, si valuta **basso** il rischio legato alla gestione dei seguenti trattamenti (identificati come da tabella 1.1, alla quale si rimanda per i dati caratteristici):

Identificativo	Descrizione di massima

(per esempio:)

DIP/01	Dati comuni dei dipendenti

Sinteticamente, si valuta **medio** il rischio legato alla gestione dei seguenti trattamenti (identificati come da tabella 1.1, alla quale si rimanda per i dati caratteristici):

trattamenti con rischio medio	
Identificativo	Descrizione di massima

Sinteticamente, si valuta **alto** il rischio legato alla gestione dei seguenti trattamenti (identificati come da tabella 1.1, alla quale si rimanda per i dati caratteristici):

trattamenti con rischio alto	
Identificativo	Descrizione di massima

(per esempio:)

DIP/01	Dati sensibili dei dipendenti (fascicoli inviati dal medico del lavoro e conservati in busta sigillata)

Di seguito sono elencati gli eventi che possono verificarsi, suddivisi in base alla natura della causa scatenante (operatori, strumenti elettronici, struttura aziendale); per ciascuno è specificato l'identificativo della contromisura, per il cui dettaglio si rimanda alla successiva sezione 19.4.

(la tabella che segue è quella predisposta dall'ufficio del Garante della privacy nella bozza dello scorso 13 maggio 2004; come indicato dal medesimo ufficio, si tratta solo di una lista esemplificativa e non esaustiva, da prendere come base di partenza per ogni utile implementazione legata alle specifiche esigenze e peculiarità di ciascun soggetto interessato alla redazione del DPS)

Tabella 3.1 - Analisi dei rischi			
Evento		**Descrizione**	**Contromisura**
Comportamenti degli operatori	Furto di credenziali di autenticazione		
	Carenza di consapevolezza, disattenzione o incuria		
	Comportamenti sleali o fraudolenti		
	Errori materiali		

Eventi relativi agli strumenti	Azione di virus informatici		
	Spamming o altre tecniche informatiche di sabotaggio		
	Malfunzionamento degli strumenti elettronici		
	Accessi esterni non autorizzati		
	Intercettazione di informazioni in rete		
Eventi relativi al contesto strutturale	Accessi non autorizzati a locali ad accesso ristretto		
	Asportazione e furto di strumenti contenenti dati		
	Eventi distruttivi, naturali o accidentali o dolosi, o per incuria		
	Guasto ai sistemi complementari (impianti elettrico, condizionamento)		
	Errori umani nella gestione della sicurezza fisica		

Regola 19.4 Misure in essere e da adottare.

A fronte dell'analisi dei rischi di cui alla precedente sezione 19.3, di seguito si descrivono le misure di sicurezza adottate dalla società (*o studio o altro*).

(di seguito si propone un esempio)

Misura 1. Antivirus. Ogni singolo computer è dotato di dispositivo antivirus, che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento antivirus, e in ogni caso almeno settimanalmente, in orario compatibile con il fatto che il computer non sia spento (in questo caso la scansione avverrà alla successiva accensione).
Misura 2. Firewall. Sul server è stato installato firewall con le seguenti caratteristiche: …
Misura 3. Backup. E' stato disposto l'obbligo di provvedere ad un backup settimanale dei dati e dei sistemi installati sul server su cd rom, i quali vengono conservati e chiusi in un armadio chiuso a chiave e protetto da agenti ignifughi, e si è data disposizione di verificare, effettuato il backup, la leggibilità del supporto e che una volta a settimana si proceda a verifica a campione della leggibilità dei dati; una volta effettuato e verificato un backup, deve essere distrutto il cd rom precedente.
Misura 4. Screensaver. Tutti gli utilizzatori di strumenti elettronici non devono lasciare incustodito, o accessibile, lo strumento stesso. A tale riguardo, per evitare errori e dimenticanze, è stato predisposto lo screensaver automatico dopo … minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
Misura 5. Autenticazione informatica. Tale misura è stata adottata dotando ciascun incaricato di una password di almeno 8 caratteri. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né alla società. La stessa viene autonomamente scelta dall'incaricato e dallo stesso custodita in una busta chiusa che viene consegnata al titolare del trattamento, il quale provvede a metterla nella cassaforte in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria password. Si è altresì disposto che le password vengano automaticamente disattivate dopo tre mesi di non utilizzo.

Misura 6. Archiviazione. Si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. I fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti.
Misura 7. Stampe centralizzate. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato dall'interessato o consegnato allo stesso.
Misura 8. Fax. I fax sono ricevuti su carta normale, e quindi è evitato il deterioramento tipico della carta chimica. I documenti arrivano in zona protetta, accessibile solo dagli incaricati dell'area della segreteria, con la parte scritta verso il basso per evitare di rimanere in vista incidentalmente.
Misura 9. Archivio. Il locale destinato all'archivio è sempre chiuso a chiave. L'incaricato preposto dovrà controllare l'accesso all'archivio. Fuori dall'orario di lavoro l'accesso all'archivio è consentito esclusivamente previa registrazione.
Misura 10. Distruzione documenti. Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica, previo passaggio nelle apposite macchine tagliadocumenti (in dotazione almeno in misura di uno per ciascun ufficio) e che detti sacchi siano chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato.
Misura 11. Eventi naturali. La società ha provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. 626/94.

Regola 19.5 Ripristino della disponibilità dei dati.

Oltre alla procedura di backup (vedasi Misura 3 della precedente sezione) la società (*o studio o altro*) ha approntato la seguente procedura di "disaster recovery", vale a dire di ripristino della disponibilità dei dati.

(di seguito si propone l'ipotesi in cui avvalendosi di consulenti informatici esterni all'azienda essi risultano coinvolti nelle procedure di sicurezza)

Si premette che ci si avvale anche della consulenza informatica della società ……., come risulta anche dalla lettera di assunzione di incarico sottoscritta in data …….

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici:
1. deve essere avvertito il titolare del trattamento dei dati e l'incaricato che ha in custodia il CD ROM di back up nonché i CD ROM contenenti i vari software installati sugli strumenti elettronici;
2. ci si deve rivolgersi immediatamente al tecnico manutentore del consulente informatico sollecitandone al più presto l'assistenza;
3. ciascun incaricato deve provvedere ad inventariare nella maniera più precisa possibile il lavoro svolto dal momento dell'ultimo back up al momento della rottura irreversibile;
4. si devono reinstallare i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel CD ROM di back up;
5. si deve provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
6. al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei dati in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato dal tecnico incaricato.

Regola 19.6 Pianificazione degli interventi formativi.

Nell'ambito delle procedure di tutela della sicurezza dei dati trattati dalla società (*o studio o altro*) si è proceduto a stila re il piano dell'impegno formativo che si prevede di sostenere in attuazione della normativa sulla privacy, secondo la tabella che segue.

Tabella 6.1 – Interventi formativi previsti					
Corso di formazione	Descrizione sintetica	Categorie interessate	Numero soggetti interessati	Incaricati già formati in preced.	Calendario date

Regola 19.7 Trattamenti affidati all'esterno.

In quest'ultima sezione vengono fornite, con l'ausilio della successiva tabella 7.1, tutte le indicazioni necessarie ad identificare i dati trattati all'esterno, nonché i soggetti coinvolti.
Si premette che è stata predisposta idonea documentazione rilasciata dai soggetti cui le varie attività sono affidate dalla quale risulta:

- che il terzo dichiara di essere consapevole che i dati da lui trattati nell'espletamento dell'incarico ricevuto sono dati personali e, come tali, sono soggetti alla disciplina di cui al D.Lgs. 196/2003 (Codice per la protezione dei dati personali);
- che il terzo dichiara di ottemperare agli obblighi previsti dal predetto D.Lgs. 196/2003;
- che il terzo dichiara di adottare ogni istruzione ricevuta dal titolare del trattamento;
- che il terzo si impegna a relazionare il titolare in ordine alle misure di sicurezza da lui adottate, notiziando il committente circa le situazioni di pericolo per i dati in cui potrebbe imbattersi;
- che il terzo dichiara di riconoscere il diritto del committente alla verifica periodica dell'applicazione delle norme di sicurezza adottate.

Tabella 7.1 – Trattamenti affidati all'esterno					
Attività esternalizzata	Descrizione sintetica	Dati sensibili e giudiziari interessati	Soggetto esterno incaricato	Descrizione criteri per l'adozione delle misure di sicurezza	Date delle verifiche

Luogo e data ***firma***