

O.d.G. del 30/03/2006

PROPOSTA DI DELIBERAZIONE PER IL CONSIGLIO DI AMMINISTRAZIONE N° 3

Deliberazione n° 10/2006

del 30/3/2006

OGGETTO DELLA PROPOSTA

Approvazione ed adozione del Documento Programmatico sulla Sicurezza (D.Lgs. 30 giugno 2003 n. 196).

Ufficio proponente: AREA INFORMATICA E STATISTICA



ALLEGATI/NOTE:

- 1) Documento Programmatico sulla Sicurezza (D.Lgs. 30 giugno 2003, n° 196).

Il Direttore Generale, d'intesa con il Direttore Amministrativo e con il Responsabile dell'Area Informatica e Statistica, riferisce e propone quanto segue:

Come è noto, in data 1 Gennaio 2004 è entrato in vigore il D.Lgs. n. 30 giugno 2003 n. 196, noto come "Codice in materia di protezione dei dati personali" o Testo Unico della privacy.

Gli uffici aziendali e, segnatamente, l'Area Informatica e Statistica, hanno già predisposto una serie di adempimenti richiesti dalla citata normativa, tra i quali l'individuazione dei Responsabili e degli Incaricati del trattamento dei dati, la predisposizione di un programma di formazione rivolto a tutto il personale interessato, nonché l'adeguamento del sistema informatico alle prescrizioni tecniche richieste dalla nuova normativa.

Uno degli obblighi più importanti previsti dal decreto in oggetto è la redazione del Documento Programmatico sulla Sicurezza, per mezzo del quale l'Azienda dichiara le misure e gli strumenti adottati, e da adottare, per garantire la tutela e la riservatezza dei dati personali di cui essa viene in possesso nello svolgimento dei compiti istituzionali.

La scadenza originaria della predisposizione del D.P.S. fu fissata al 30/06/2004, ma una serie di proroghe l'ha fatta più volte slittare, fissandola, da ultimo, al prossimo 31 marzo 2006.

Affinché assuma valenza legale, il Documento Programmatico sulla Sicurezza deve avere

data certa, per cui se ne rende opportuna la formale approvazione da parte del Consiglio di Amministrazione.

Il Responsabile dell'Area Informatica e Statistica

Il Direttore Amministrativo

Il Direttore Generale

IL CONSIGLIO DI AMMINISTRAZIONE

- vista la proposta
- visto lo Statuto della Società;
- considerata condivisibile la proposta;
- a voti

DELIBERA

- 1) Di approvare il Documento Programmatico sulla Sicurezza, allegato alla presente delibera per formarne parte integrante e sostanziale.
- 2) Di delegare il Presidente del C.d.A. ad approvare le eventuali modifiche che si rendessero in futuro necessarie per adeguare il D.P.S. a nuove e/o mutate esigenze o a modificazioni della struttura aziendale.

N° 10 del Registro

DELIBERAZIONE DEL CONSIGLIO DI AMMINISTRAZIONE

n° 10 del 30.03.2006

OGGETTO

D.Lgs. 196/2003 – NUOVO CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI. DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (D.P.S.): APPROVAZIONE.

L'anno duemilasei, il giorno 30 (trenta) del mese di Marzo, alle ore 9.15, in Taranto e nella sede della Società, si è riunito in seduta ordinaria, previo avviso di convocazione, il Consiglio di Amministrazione nelle persone dei Signori:

1) Enzo	MANCO	Presidente	
2) Saverio	CREAZZO	Vice Presidente	(ass.)
3) Giuseppe	BIANCO	Componente	
4) Antonio	CITREA	Componente	(ass.)
5) Antonio	RANUCCI	Componente	
6) Marina	RIBERTI	Componente	
7) Ugo	TRONCONE	Componente	(ass.)

Svolge le funzioni di Segretario del Consiglio il Dott. Cosimo Rochira.

Il Presidente, constatato il numero legale degli intervenuti, dichiara valida e aperta la seduta.

Il Direttore Generale, d'intesa con il Direttore Amministrativo e con il Responsabile dell'Area Informatica e Statistica, riferisce e propone quanto segue:

- Come è noto, in data 1 Gennaio 2004 è entrato in vigore il D.Lgs. n. 30 giugno 2003 n. 196, noto come "Codice in materia di protezione dei dati personali" o Testo Unico della privacy.
- Gli uffici aziendali e, segnatamente, l'Area Informatica e Statistica, hanno già predisposto una serie di adempimenti richiesti dalla citata normativa, tra i quali l'individuazione dei Responsabili e degli Incaricati del trattamento dei dati, la predisposizione di un programma di formazione rivolto a tutto il personale interessato, nonché l'adeguamento del sistema informatico alle prescrizioni tecniche richieste dalla nuova normativa.
- Uno degli obblighi più importanti previsti dal decreto in oggetto è la redazione del Documento Programmatico sulla Sicurezza, per mezzo del quale l'Azienda dichiara le misure e gli strumenti adottati, e da adottare, per garantire la tutela e la riservatezza dei dati personali di cui essa viene in possesso nello svolgimento dei compiti istituzionali.
- La scadenza originaria della predisposizione del D.P.S. fu fissata al 30/06/2004, ma una serie di proroghe l'ha fatta più volte slittare, fissandola, da ultimo, al prossimo 31 marzo 2006.
- Affinché assuma valenza legale, il Documento Programmatico sulla Sicurezza deve avere data certa, per cui se ne rende opportuna la formale approvazione da parte del Consiglio di Amministrazione.

F.to Il Responsabile dell'Area Informatica - Dott. Ciro Russo

F.to Il Direttore Amministrativo - Dott. Pietro Carallo

F.to Il Direttore Generale - Ing. Giovanni Matichecchia

IL CONSIGLIO DI AMMINISTRAZIONE

- vista la proposta;
- visti lo Statuto della Società ed il Codice Civile;
- ritenuto di dover provvedere in merito;

a voti unanimi, resi nelle forme di legge

DELIBERA

- 1) Di approvare il Documento Programmatico sulla Sicurezza che allegato alla presente delibera ne costituisce parte integrante e sostanziale.
- 2) Di delegare il Presidente del C.d.A. ad approvare le eventuali modifiche che si rendessero in futuro necessarie per adeguare il D.P.S. a nuove e/o mutate esigenze ovvero a modificazioni della struttura aziendale.

l.c.s.

firmato: **IL SEGRETARIO**
Dr. Cosimo Rochira

firmato: **IL PRESIDENTE**
Enzo Manco

Documento

Programmatico sulla

Sicurezza

INDICE (estratto dal DPS)

(Art. 34 e regola 19 dell'allegato B del codice in materia di protezione dei dati personali)

25 ottobre 2004

1. Premessa al DPS	3
1.1 Elenco delle revisioni	3
1.2 Definizioni (art. 4 Dlgs 196/2003)	3
1.3 Informazioni contenute	5
2. Documento Programmatico sulla Sicurezza	6
2.1 Sedi del Cliente	6
2.2 Organigramma aziendale	7
2.3 Schema della struttura fisica e logica del sistema informativo	8
3. Elenco dei trattamenti di dati personali (Regola 19.1)	9
3.1 Tipologie dei dati trattati	9
3.2 Schede analitiche dei Trattamenti	10
3.3 Mappa dei Trattamenti	12
3.4 Elenco dei Trattamenti: descrizione degli strumenti utilizzati	13
3.5 Aree, locali e strumenti con i quali si effettuano i trattamenti	13
3.6 Trattamenti affidati all'esterno (Regola 19.7)	14
4. Distribuzione dei compiti e delle responsabilità (Regola 19.2)	15
4.1 Titolare	15
4.2 Responsabili del trattamento	15
4.3 Unità operative ed incaricati del trattamento	17
4.4 Mansionario Privacy	18
5. Analisi dei rischi che incombono sui dati (Regola 19.3)	20
6. Misure da adottare ed in essere (Regola 19.4)	29
6.1 Controllo generale sullo stato della sicurezza.	34
7. Criteri e modalità di ripristino della disponibilità dei dati (Regola 19.5)	35
7.1 Scheda descrittiva delle misure adottate	36
7.2 La protezione di aree e locali	37
7.3 Custodia e archiviazione dei dati	37
7.4 Misure logiche di sicurezza	37
8. Scadenario delle misure da adottare	38
9. Pianificazione degli interventi formativi (Regola 19.6)	38
9.1 Pianificazione degli interventi formativi previsti	38
10. Dichiarazioni d'impegno e firma	39

1. Premessa al DPS

1.1 Elenco delle revisioni

Versione Data Nota

Versione Bozza 13.09.2004 Bozza della prima stesura

Versione sottoposta al vaglio 28.09.2004 Seconda stesura dopo l'audit del 1 settembre 2004

1.2 Definizioni (art. 4 Dlgs 196/2003)

1. Ai fini del presente documento si intende per:

- a) **"trattamento"**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- b) **"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;
- c) **"dati identificativi"**, i dati personali che permettono l'identificazione diretta dell'interessato;
- d) **"dati sensibili"**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- e) **"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;
- f) **"titolare"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- g) **"responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- h) **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- i) **"interessato"**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- j) **"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;
- k) **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- l) **"dato anonimo"**, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- m) **"blocco"**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- n) **"banca di dati"**, qualsiasi complesso organizzato di dati personali, ripartito in una più unità dislocate in uno o più siti;
- o) **"Garante"**, l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente documento si intende, inoltre, per:

- a) **"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 collegate ad un abbonato o utente ricevente, identificato o identificabile;
- a) **"chiamata"**, la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- b) **"reti di comunicazione elettronica"**, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la

diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

- c) **"rete pubblica di comunicazioni"**, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- d) **"servizio di comunicazione elettronica"**, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- e) **"abbonato"**, qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- f) **"utente"**, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- g) **"dati relativi al traffico"**, qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- i) **"dati relativi all'ubicazione"**, ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- h) l) **"servizio a valore aggiunto"**, il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- i) **"posta elettronica"**, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente documento si intende, altresì, per:

- a) **"misure minime"**, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- b) **"strumenti elettronici"**, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- c) **"autenticazione informatica"**, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- d) **"credenziali di autenticazione"**, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- e) **"parola chiave"**, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- f) **"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;
- g) **"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.

4. Ai fini del presente documento si intende per:

- h) **"scopi storici"**, le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- i) **"scopi statistici"**, le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- j) **"scopi scientifici"**, le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Infine, ai soli fini del presente documento, s'intenderà con la parola **"Interazione"** il significato di connessione tra uno strumento non elettronico e l'essere umano.

1.3 Informazioni contenute

L'obbligo di redazione de "Il documento programmatico sulla sicurezza (Dps)", ai sensi dell'articolo 34 del codice, è vincolante per quei soggetti che trattano dati personali attraverso l'uso di strumenti elettronici. Conformemente a quanto prescrive il punto 19 del Disciplinare Tecnico, allegato sub b) al Dlgs 196/2003, nel presente documento si forniscono le necessarie informazioni per costituire il DPS riguardanti:

- l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare tecnico), illustrazione della "mappa dei trattamenti".
- la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati; costituzione ed aggiornamento del "mansionario privacy", (punto 19.2)
- l'analisi dei rischi che incombono sui dati (19.3)
- le misure da adottare, per garantire l'integrità e la disponibilità dei dati (19.4). Vengono altresì indicate le misure in essere per ridurre al minimo i rischi individuati.
- i criteri e le modalità di ripristino dei dati allorché si fosse verificato uno dei rischi menzionati (19.5)
- la previsione di interventi formativi degli incaricati del trattamento (19.6)
- i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno (19.7)

Particolare attenzione è posta a quei trattamenti che coinvolgono anche dati sensibili o giudiziari, a tal proposito nel presente documento vengono nel dettaglio descritte, qualora necessario, le misure minime richieste dal medesimo disciplinare, di seguito indicate:

- Modifiche della parola chiave almeno ogni tre mesi (5)
- Aggiornamenti almeno semestrali dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti (nel seguito del documento indicati come "Patch"). (17)
- Individuazione dei criteri da adottare per la cifratura o per la separazione (disgiunzione) di particolari dati sensibili (vita sessuale, stato di salute e genetici) da quelli personali, relativamente all'interessato (19.8 e 24)
- Misure contro l'accesso abusivo (20)
- Misure per la custodia e uso dei supporti rimuovibili (21 e 22)
- Misure per il ripristino accesso ai dati (23)

Altresì per meglio comprendere la struttura dell'organizzazione in esame sono illustrati sia lo schema della struttura fisica e logica del sistema informativo, sia l'organigramma aziendale in adozione presso questa Società.

Infine il documento si dipana disponendo i contenuti con impostazione orizzontale per favorire la lettura delle numerose tabelle che tendono a svilupparsi in senso longitudinale.

2. Documento Programmatico sulla Sicurezza

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato da A.M.A.T. S.p.A. (nel seguito del documento indicato come Titolare).

=====

Il presente documento è redatto e firmato in calce dal responsabile per la sicurezza, i cui dati sono i seguenti:

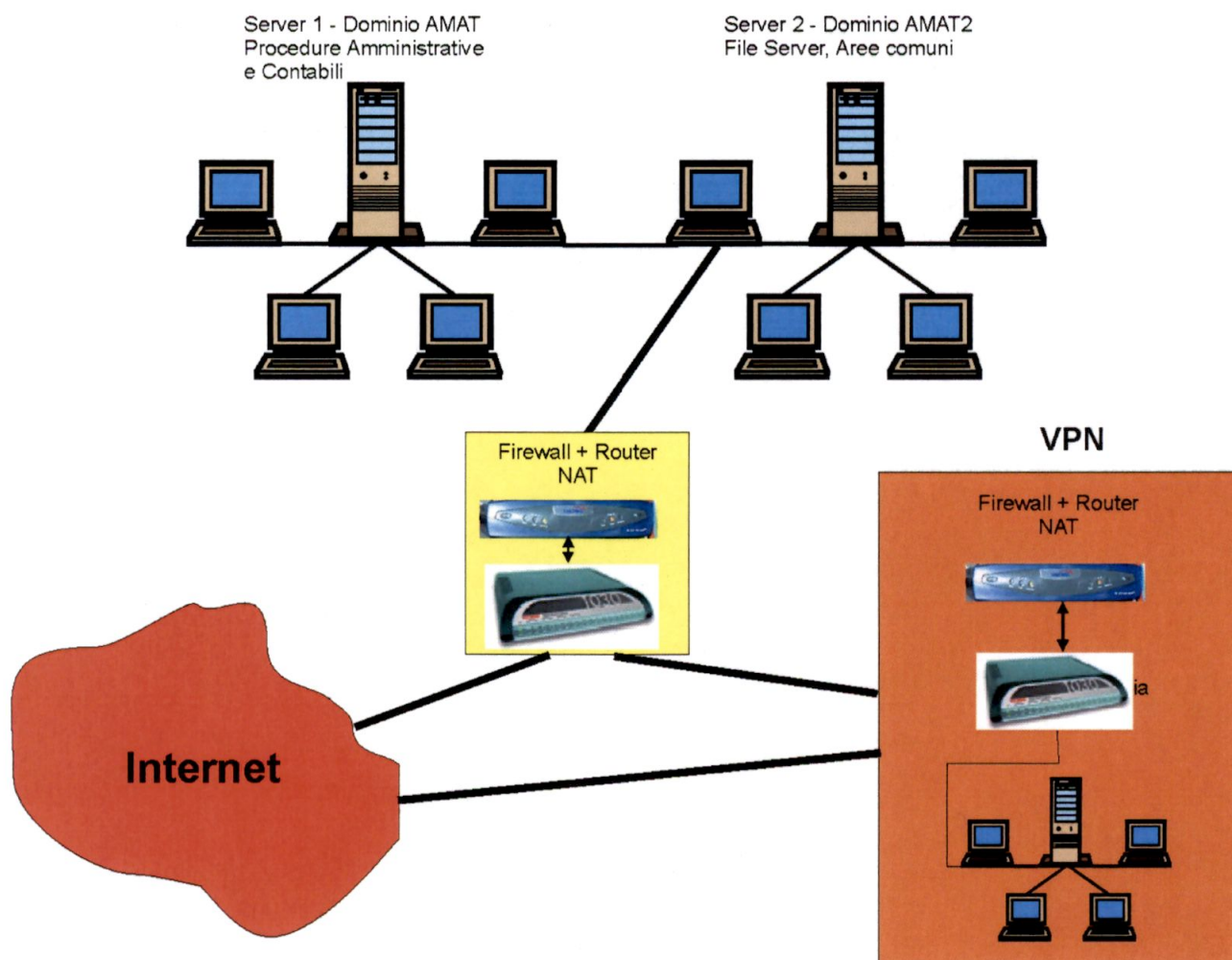
- **Ciro Russo**, Responsabile Area Informatica nominato con lettera del.....(se persona fisica interna all'organizzazione)

2.1 Sedi del Cliente

Sede	Indirizzo	Tipo Sede
Sede	Via Cesare Battisti, 657	Unica

2.2 Organigramma aziendale

2.3 Schema della struttura fisica e logica del Sistema Informativo



3. Elenco dei trattamenti di dati personali (Regola 19.1)

3.1 Tipologie di dati trattati

A seguito dell'analisi compiuta si sono identificati i seguenti trattamenti:

- Dati relativi al personale o ai candidati per diventarlo, di natura anche sensibile
- Dati comuni relativi a clienti e fornitori
- Dati relativi allo svolgimento di attività economiche e commerciali
- Dati anche sensibili indispensabili allo svolgimento dell'attività professionale per assolvere a obblighi normativi e contrattuali

3.2 Schede analitiche dei trattamenti.

T01	
Descrizione	Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture
Natura dei dati	DATI COMUNI su Fornitori e Clienti: Dati contabili, ordini, bolle di spedizione, fatture, articoli Nome, cognome, età, sesso, luogo e data di nascita
Struttura di riferimento	Ufficio Ragioneria, Magazzino, Ufficio Contratti e Acquisti, Area contabilità, Ufficio tecnico
Strumenti	Elaboratori in rete locale: Personal Computer (nr. XX), Server1 (dominio AMAT) Programmi per elaboratore: Oceano (Pluservice S.r.l.)
Banche dati	SQL Server
Locali	Dove avviene il Trattamento: Ufficio Ragioneria, Magazzino, Ufficio Contratti e Acquisti, Area contabilità, Ufficio tecnico

T02	
Descrizione	Finalità amministrativo contabili: Gestione Officina
Natura dei dati	DATI COMUNI su Personale dipendente: Nome, cognome, Matricola aziendale
Struttura di riferimento	Ufficio Tecnico
Strumenti	Elaboratori in rete locale: Personal Computer (nr. XX), Server1 (dominio AMAT) Programmi per elaboratore: Officina 2000 (Pluservice S.r.l.)
Banche dati	SQL Server
Locali	Dove avviene il Trattamento: Ufficio tecnico

T03	
Descrizione	Finalità amministrativo contabili: Trattamento giuridico ed economico del personale - calcolo e pagamento di retribuzioni ed emolumenti vari
Natura dei dati	DATI COMUNI su Personale dipendente: Indirizzo privato, indirizzo di lavoro, numero di telefono, di telefax o di posta elettronica Nome, cognome, età, sesso, luogo e data di nascita Numero di posizione previdenziale o assistenziale, qualifica, livello, matricola aziendale Retribuzioni, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente Stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare
Struttura di riferimento	Ufficio Ragioneria, Ufficio Retribuzioni
Strumenti	Elaboratori in rete locale: Personal Computer (nr. XX), Server1 (dominio AMAT) Programmi per elaboratore: Sispac (OSRA paghe)
Banche dati	COBOL
Locali	Dove avviene il Trattamento: Ufficio Ragioneria, Ufficio Retribuzioni

T04	
Descrizione	Finalità amministrativo contabili: Rilevazione Presenze
Natura dei dati	DATI COMUNI su Personale dipendente Nome, cognome, età, sesso, luogo e data di nascita, matricola aziendale
Struttura di riferimento	Ufficio Retribuzioni
Strumenti	Personal Computer (nr. 1) in rete locale Programmi per elaboratore: Copernico (OSRA paghe)
Banche dati	ORACLE
Locali	Dove avviene il Trattamento: Ufficio Retribuzioni

T05

Descrizione	Finalità amministrativo contabili: Gestione degli introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)
Natura dei dati	DATI COMUNI su cittadini: Indirizzo, numero di telefono, Nome, cognome, età, sesso, luogo e data di nascita
Struttura di riferimento	Ufficio Prodotti del Traffico
Strumenti	Personal Computer (nr. 3) in rete locale Programmi per elaboratore: Introiti (Pluservice S.r.l.)
Banche dati	Open Access
Locali	Dove avviene il Trattamento: Ufficio Prodotti del Traffico

T06

Descrizione	Finalità amministrativo contabili: Archivio dipendenti
Natura dei dati	DATI COMUNI su Personale dipendente: Indirizzo privato, indirizzo temporaneo, numero di telefono Nome, cognome, età, sesso, luogo e data di nascita, qualifica, avanzamenti di carriera, giorni malattia, matricola aziendale
Struttura di riferimento	Ufficio Retribuzioni, Area Personale
Strumenti	Personal Computer (nr. 3) in rete locale Programmi per elaboratore: Archivio Personale
Banche dati	Filemaker Pro
Locali	Dove avviene il Trattamento: Ufficio Retribuzioni, Area Personale

T07

Descrizione	Finalità amministrativo contabili: Archivio Sinistri
Natura dei dati	DATI COMUNI su Personale dipendente: Indirizzo privato, numero di telefono Nome, cognome, età, luogo e data di nascita, qualifica, matricola aziendale Numero, tipo e data scadenza patente DATI COMUNI su cittadini: Indirizzo, Compagnia Assicurativa, Nome, Cognome
Struttura di riferimento	Ufficio Sinistri, Unità Pubbliche Relazioni
Strumenti	Personal Computer (nr. 2) in rete locale Programmi per elaboratore: Sinistri
Banche dati	Filemaker Pro
Locali	Dove avviene il Trattamento: Ufficio Sinistri, Unità Pubbliche Relazioni

T08

Descrizione	Finalità amministrativo contabili: Multe
Natura dei dati	DATI COMUNI su Personale dipendente: Nome, cognome, matricola aziendale DATI COMUNI su cittadini: Indirizzo, Nome, Cognome, Data e luogo di Nascita, Età, Sesso, Occupazione
Struttura di riferimento	Ufficio Prodotti del Traffico; Segreteria Ufficio Movimento (solo inserimento dati)
Strumenti	Personal Computer (nr. 2) in rete locale presso la sede in Via Cesare Battisti n. 657 Personal Computer (nr. 2) in rete locale presso l'Ufficio Prodotti del traffico Programmi per elaboratore: Multe
Banche dati	Filemaker Pro
Locali	Dove avviene il Trattamento: Ufficio Prodotti del Traffico

T09	
Descrizione	Finalità amministrativo contabili: Movimento
Natura dei dati	DATI COMUNI su Personale dipendente: Nome, cognome, matricola aziendale, gruppo di rotazione, turnazione
Struttura di riferimento	Area Movimento
Strumenti	Personal Computer (nr. 7) in rete locale presso la sede in Via Cesare Battisti n. 657 Programmi per elaboratore: Movimento
Banche dati	SQL SERVER
Locali	Dove avviene il Trattamento: Area Movimento

T10	
Descrizione	Finalità amministrativo contabili: Concorso autisti
Natura dei dati	DATI COMUNI su Cittadini Indirizzo, Nome, Cognome, Data e luogo di Nascita, Età, Sesso
Struttura di riferimento	Ufficio Prodotti del Traffico; Segreteria Ufficio Movimento (solo inserimento dati)
Strumenti	Personal Computer (nr. 2) in rete locale presso la sede in Via Cesare Battisti n. 657 Programmi per elaboratore: Concorso
Banche dati	Filemaker Pro
Locali	Dove avviene il Trattamento: Ufficio Segreteria

3.3 Mappa dei trattamenti

Strumenti	DATI COMUNI Fornitori e Clienti	DATI COMUNI Personale dipendente	DATI COMUNI Persone fisiche	DATI SENSIBILI Personale dipendente
Armadi e/o Schedari nella struttura di riferimento	T01	T03		T03
Software OCEANO (Pluservice S.r.l.)	T01			
Software OFFICINA 2000 (Pluservice S.r.l.)		T02		
Software MOVIMENTO (Pluservice S.r.l.)		T02		
Software SISPAC (Pluservice S.r.l./OSRA paghe)		T02		
Software INTROITI (Pluservice S.r.l.)			T05	
Software COPERNICO (Pluservice S.r.l./OSRA paghe)		T02		
Archivio Personale (A.M.A.T. S.p.A.)		T06		T06
Archivio Sinistri (A.M.A.T. S.p.A.)		T07	T07	
Archivio Multe (A.M.A.T. S.p.A.)			T08	
Archivio Concorso			T10	

3.4 Elenco dei trattamenti: descrizione degli strumenti utilizzati.

Identificativo del trattamento	Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
T01	AMAT_EURO AMATSQL AMATSTORICI APINFO	SERVER SEDE(ex cabina di trasformazione) COPIE SICUREZZA Cassaforte ignifuga (locale cassette economato) Cassaforte ignifuga (Area Informatica)	PC	Rete locale
T02 T09	AMATPLUS			
T03	Archivio anagrafico dipendenti e tabelle di gestione			
T07	Sinistri_ e tabelle correlate			
T05	Introiti e tabelle correlate			
T08	Ve_dacon, Ve_dacon_2002 e tabelle correlate			
T06	Anagrafica dipendenti e tabelle correlate			
T10	Selezione Conducenti			
T04	GW2000	PC retribuzioni COPIE SICUREZZA SERVER	PC	PC locale
Biglietteria	Data base utenti, titoli di viaggio e tabelle correlate	Via Matteotti ang. Via Margherita COPIE SICUREZZA CD settimanali	PC	Rete locale
Data di aggiornamento: 14/06/2004				

3.5 Aree, locali e strumenti con i quali si effettuano i trattamenti

Il trattamento dei dati avviene nella sede e luogo di lavoro, situata in Via Cesare Battisti n. 657 e in seguito denominata SEDE.

Gli uffici sono dislocati al primo piano, l'accesso all'Azienda per gli esterni è controllato da servizio di sorveglianza tramite Guardie Giurate previa presentazione di documento d'identità ed autorizzazione all'accesso da parte dell'ufficio di destinazione; inoltre l'accesso agli uffici dell'Amministrazione è controllato da personale interno, mediante porta in anticorodal con apertura controllata elettricamente ed identificazione a mezzo videocitofono.

Un ulteriore trattamento dei dati avviene nel luogo di lavoro, situato in Via D'Aquino n. 21, in seguito denominata UFFICIO.

L'UFFICIO è dislocato al piano terra, l'accesso è controllato da Guardia Giurata; nell'UFFICIO è installato un sistema di video sorveglianza mediante telecamere a circuito chiuso, installate nell'ingresso, nella sala di attesa e nella sala biglietteria. Le telecamere trasmettono ciclicamente le immagini su un monitor installato nell'ingresso per consentire alla Guardia Giurata di controllare i locali su menzionati. Il sistema effettua inoltre una registrazione su videocassette VHS di quanto ripreso dalle telecamere; le video cassette vengono sostituite giornalmente e sovrascritte con periodicità settimanale. Nell'ufficio è installato inoltre un sistema di allarme per incendio e per tentativi di effrazione, dotato di combinatore telefonico, che, in caso di allarme, contatta le forze dell'ordine ed i responsabili dell'Azienda.

A - Schedari e altri supporti cartacei

I supporti cartacei sono raccolti in schedari a loro volta custoditi come segue:

- Archivio **CARTELLE CLINICHE DIPENDENTI** localizzato in SEDE presso l'ufficio del Medico competente, conservate in apposito armadio dotato di chiusura con chiave in possesso del Medico Competente; al locale accedono solo i dipendenti, quando convocati dal Medico; la documentazione relativa ai dipendenti viene prelevata dal Medico per il tempo necessario allo svolgimento del trattamento e, al termine, riposta nell'armadio.

- Archivio **CARTELLE PERSONALI DIPENDENTI** localizzato in SEDE presso l'Ufficio Retribuzioni, conservate in appositi armadi dotati di chiusura con chiave in possesso del personale dell'ufficio; al locale accedono solo le persone autorizzate; la documentazione viene prelevata dal personale dell'ufficio per il tempo necessario allo svolgimento del trattamento e, al termine, riposta nell'armadio.
- Archivio **SINISTRI** localizzato in SEDE presso l'Ufficio Retribuzioni, conservate in apposito armadio dotato di chiusura con chiave in possesso del personale dell'ufficio; al locale accedono solo le persone autorizzate; la documentazione viene prelevata dal personale dell'ufficio per il tempo necessario allo svolgimento del trattamento e, al termine, riposta nell'armadio.
- Archivio **DOCUMENTAZIONE INVALIDITA' PER EMISSIONE ABBONAMENTI GRATUITI** localizzato in SEDE presso l'Unità Pubbliche Relazioni, conservate in apposito armadio dotato di chiusura con chiave in possesso del Responsabile dell'Unità; al locale accedono solo le persone autorizzate; la documentazione viene prelevata dal Responsabile dell'Unità per il tempo necessario allo svolgimento del trattamento e, al termine, riposta nell'armadio.
- Archivio **VERBALI MULTE ED ORDINANZE DI INGIUNZIONE** localizzato presso l'Ufficio Prodotti del Traffico, in Via D'Aquino n. 21, conservate in appositi armadi dotati di chiusura con chiave in possesso del personale dell'ufficio; al locale accedono solo le persone autorizzate; la documentazione viene prelevata dal personale dell'ufficio per il tempo necessario allo svolgimento del trattamento e, al termine, riposta nell'armadio.
- Archivio **AUTOCERTIFICAZIONI PER EMISSIONE ABBONAMENTI** localizzato presso l'Ufficio Prodotti del Traffico, in Via D'Aquino n. 21, conservate in appositi armadi dotati di chiusura con chiave in possesso del personale dell'ufficio; al locale accedono solo le persone autorizzate; la documentazione viene prelevata dal personale dell'ufficio per il tempo necessario allo svolgimento del trattamento e, al termine, riposta nell'armadio.

• *ARCHIVIO STORICO*

B - Elaboratori non in rete

Non sono presenti postazioni fisse non accessibili da altri elaboratori.

C - Elaboratori in rete privata

Il sistema di lavoro della struttura avviene con elaborazione in rete privata.

Si dispone di una rete, realizzata mediante collegamenti via cavo costituita da:

- n 2 server, localizzati nell'area ufficio, nel locale ex cabina di trasformazione, protetta da porta in ferro con serratura.
- n 40 postazioni lavoro dislocate nell'area SEDE
- n 6 postazioni lavoro dislocate nell'area UFFICIO
- n 22 stampanti di cui n 9 laser dislocate nell'area SEDE
- n 4 stampanti di cui n 1 laser dislocate nell'area UFFICIO
- n 7 fax localizzati nell'area SEDE
- n 1 fax localizzato nell'area UFFICIO
- n 2 dispositivi di backup localizzato nell'area ufficio, integrati nei server.

** Nessun armadio con
chiavi*

** non sono suff. di
armadi*

D - Elaboratori in rete pubblica

Non è presente una struttura che utilizza reti di telecomunicazione pubbliche.

E - Impianti di video-sorveglianza

Non sono utilizzati impianti di video-sorveglianza

3.6 Trattamenti affidati all'esterno (Regola 19.7)

Trattamento	Soggetto esterno	Natura dei dati	Garanzie
TE01 - Manutenzione Procedure Applicative (T01 - T02 - T03 - T04 - T05 - T09)	Pluservice S.r.l.	DATI COMUNI	Adempimento degli obblighi previsti dal codice per la protezione dei dati personali

4. Distribuzione dei compiti e delle responsabilità (Regola 19.2)

Titolare del trattamento dei dati

In questa sezione si descrive l'organizzazione della struttura in esame, riguardo ai trattamenti effettuati dal Titolare, dagli Incaricati e dai Responsabili qualora nominati.

Il trattamento dei dati personali è eseguito solo da soggetti che hanno ricevuto un formale incarico, mediante documentata preposizione di ogni persona ad un'unità operativa, per la quale sia stato in precedenza individuata per iscritto l'ambito del trattamento.

4.1 Titolare

Titolare
A.M.A.T. S.p.A.

4.2 Responsabili del trattamento

Per il trattamento dei dati personali il titolare ha nominato i seguenti responsabili attribuendo loro incarichi di ordine organizzativo e direttivo, come segue:

Struttura	Responsabile	Trattamenti operati dalla struttura	Compiti della struttura
Contabilità e Bilancio	Francesco Iervoglino	Gestione contabilità ordinaria e IVA	Aggiornamento contabilità ordinaria, IVA, emissione ordinativi di pagamento e incasso, redazione Bilancio
Personale	Maria Fabiola Mennenti	Gestione Retribuzioni, Presenza, Personale	Inserimento e variazione dati anagrafici e retributivi, elaborazione stipendi, elaborazione modulistica fiscale (770 – CUD), Gestione presenza dei dipendenti, Gestione cartella personale
Informatica	Ciro Russo	Manutenzione Sistema Informativo e Procedure realizzate internamente	Aggiornamento Sistemi Operativi, Realizzazione e modifica Procedure ad uso interno, Backup Archivi, Privacy
Ufficio Prodotti del Traffico	Nicola Carrieri	Gestione magazzino titoli di viaggio e multe emesse ai viaggiatori	Distribuzione biglietti a Rivendite e pubblico, emissione di abbonamenti, emissione notifiche per multe, incasso multe
Pubbliche Relazioni	Tiziana Tursi	Gestione sinistri, rapporti con assicurazioni	Aggiornamento archivio sinistri, denuncia alle assicurazioni, rapporti con il pubblico
Segreteria	Cosimo Russo	Gestione Corrispondenza in entrata e in uscita, segreteria Presidenza e Consiglio di Amministrazione	Protocollo della Corrispondenza in entrata ed in uscita, trasmissione ordini ai fornitori, redazione di Delibere del Presidente/Consiglio di Amministrazione, distribuzione corrispondenza ed Ordini di Servizio
Magazzino	Bruno Ancarola	Gestione del Magazzino	Carico e scarico di magazzino, approvvigionamenti, emissione ordini per ricostruzione scorte
Contratti e acquisti	Bruno Ancarola	Gestione Acquisti extra scorta, contratti di fornitura, rapporti con i fornitori	Emissione ordini per approvvigionamenti non da scorte, formulazione gare di appalto, rapporti con i fornitori
Officina	Pietro Rizzo	Gestione parco automezzi, manutenzione programmata e straordinaria, richieste di acquisto	Carico/Scarico gasolio, apertura/chiusura commesse di lavorazione per riparazioni da manutenzione programmata e straordinaria, emissione richieste di acquisto
Movimento	Giuseppe Ferrante	Gestione della turnazione autisti e superiori di linea, emissione di consuntivi periodici	Programmazione e sviluppo turnazione autisti, aggiornamento situazione servizio in tempo reale, consuntivazione chilometri e presenza per retribuzioni
Pluservice S.r.l.	Pluservice S.r.l.	Manutenzione Applicativi	Aggiornamento, Modifica, Personalizzazione delle Procedure Applicative, Individuazione e Rimozione di anomalie

4.3 Unità operative ed incaricati del trattamento

Incaricato	Unità operativa	Incarico
Giuseppe Di Corrado	Ufficio Ragioneria	Incaricato del trattamento
Ettore Angiulli	Ufficio Ragioneria	Incaricato del trattamento
Vincenzo Greco	Ufficio Ragioneria	Incaricato del trattamento
Giuseppe Cardellicchio	Ufficio Ragioneria	Incaricato del trattamento
Lorenzo Stasolla	Ufficio Segreteria	Incaricato del trattamento
Enrico Picchi	Ufficio Retribuzioni	Incaricato del trattamento
Giovanni Cellammare	Ufficio Retribuzioni	Incaricato del trattamento
Giuseppe Fornaro	Ufficio Retribuzioni	Incaricato del trattamento
Amedeo Massari	Ufficio Retribuzioni	Incaricato del trattamento
Cosimo Cigliese	Ufficio Contratti e Acquisti	Incaricato del trattamento
Stefano Rota	Ufficio Contratti e Acquisti	Incaricato del trattamento
Roberto Conte	Ufficio Contratti e Acquisti	Incaricato del trattamento
Vito Di Taranto	Ufficio Magazzino	Incaricato del trattamento
Antonio Battista	Ufficio Magazzino	Incaricato del trattamento
Giuseppe Barbaro	Ufficio Magazzino	Incaricato del trattamento
Angelo De Vietro	Magazzino Distribuzione	Incaricato del trattamento
Semeraro Francesco	Magazzino Distribuzione	Incaricato del trattamento
Cosimo Zaccaria	Magazzino Distribuzione	Incaricato del trattamento
Vincenzo Rochira	Ufficio Tecnico	Incaricato del trattamento
Gregorio Paurini	Ufficio Tecnico	Incaricato del trattamento
Francesco Andrioli	Ufficio Tecnico	Incaricato del trattamento
Cosimo Massaro	Ufficio Tecnico	Incaricato del trattamento
Giuseppe D'Addario	Ufficio Programmi e Turni	Incaricato del trattamento
Giuseppe Tommaselli	Ufficio Programmi e Turni	Incaricato del trattamento
Francesco Stanisci	Ufficio Programmi e Turni	Incaricato del trattamento
Raffaele Sallustio	Ufficio Programmi e Turni	Incaricato del trattamento
Francesco Fanelli	Ufficio Programmi e Turni	Incaricato del trattamento
Pietro Rizzo	Addetti Movimento e Traffico	Incaricato del trattamento
Luciano Picuno	Addetti Movimento e Traffico	Incaricato del trattamento
Giuseppe Cappellano	Addetti Movimento e Traffico	Incaricato del trattamento
Luca Lorè	Addetti Movimento e Traffico	Incaricato del trattamento
Francesco Pignatale	Addetti Movimento e Traffico	Incaricato del trattamento
Giuseppe Monelli	Addetti Movimento e Traffico	Incaricato del trattamento
Antonio Troncone	Addetti Movimento e Traffico	Incaricato del trattamento
Nicola Laviola	Addetti Movimento e Traffico	Incaricato del trattamento
Emilio Mancini	Addetti Movimento e Traffico	Incaricato del trattamento
Rosario Sportelli	Addetti Movimento e Traffico	Incaricato del trattamento
Giovanni Vasco	Addetti Movimento e Traffico	Incaricato del trattamento
Paolo Sagliocca	Ufficio Prodotti del Traffico	Incaricato del trattamento
Pietro Vecchio	Ufficio Prodotti del Traffico	Incaricato del trattamento
Giovanni Carrino	Ufficio Prodotti del Traffico	Incaricato del trattamento
Giuseppe Pellicoro	Ufficio Prodotti del Traffico	Incaricato del trattamento
Donato Bernardi	Ufficio Prodotti del Traffico	Incaricato del trattamento
Cosimino Santoro	Ufficio Prodotti del Traffico	Incaricato del trattamento

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati
- modalità di custodia ed utilizzo dei supporti rimovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono; esse vengono allegate al presente documento.

Periodicamente, con cadenza almeno annuale, si aggiorna la definizione dei dati cui gli incaricati sono autorizzati ad accedere e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione è compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

4.4 Mansionario Privacy

Il "Mansionario Privacy" illustra sinteticamente a quali unità operative facciano capo determinati trattamenti, al fine di individuare istantaneamente quali siano i gradi di maggiore responsabilità, adottati presso questa Società.

Il Mansionario Privacy tiene conto dei trattamenti che vengono effettuati attraverso unità operative esterne, ciò viene evidenziato illustrando separatamente prima le unità operative interne e poi quelle esterne

- **Unità operativa:** riporta le indicazioni delle strutture principali o secondarie che operano un determinato trattamento
- **Compiti e responsabilità:** descrive quanto di competenza della relativa unità operativa
- **Trattamenti:** indica i codici-trattamento di competenza di ciascuna unità e la natura dei dati trattati, rispetto alla tipologia ed alla categoria di soggetti interessati.

Unità Operativa	Compiti e Responsabilità	Trattamenti
Area Informatica	Manutenzione Sistema Informativo	
Ufficio Contratti e Acquisti	Emissione ordini per approvvigionamenti non da scorte, formulazione gare di appalto, rapporti con i fornitori	T01 DATI COMUNI
Ufficio Ragioneria	Aggiornamento contabilità ordinaria, IVA, emissione ordinativi di pagamento e incasso	T01 DATI COMUNI
Ufficio Retribuzioni	Inserimento e variazione dati anagrafici e retributivi, elaborazione stipendi, elaborazione modulistica fiscale (770 – CUD), Gestione presenza dei dipendenti, Gestione cartella personale	T03 DATI COMUNI E SENSIBILI T04 DATI COMUNI T06 DATI COMUNI E SENSIBILI
Ufficio Segreteria	Protocollo della Corrispondenza in entrata ed in uscita, trasmissione ordini ai fornitori, redazione di Delibere del Presidente/Consiglio di Amministrazione, distribuzione corrispondenza ed Ordini di Servizio	T10 DATI COMUNI

Unità Operativa	Compiti e Responsabilità	Trattamenti
Ufficio Tecnico	Carico/Scarico gasolio, apertura/chiusura commesse di lavorazione per riparazioni da manutenzione programmata e straordinaria, emissione richieste di acquisto	T02 DATI COMUNI
Ufficio Turni e Programmi	Programmazione e sviluppo turnazione autisti, aggiornamento situazione servizio in tempo reale, consuntivazione chilometri e presenza per retribuzioni	T09 DATI COMUNI
Addetti al Movimento e Traffico	Aggiornamento situazione servizio in tempo reale	T09 DATI COMUNI
Ufficio Sinistri	Aggiornamento archivio sinistri, denuncia alle assicurazioni, rapporti con il pubblico	T07 DATI COMUNI
Ufficio Magazzino	Carico e scarico di magazzino, approvvigionamenti, emissione ordini per ricostituzione scorte	T01 DATI COMUNI
Magazzino Ricambi	Consultazione archivio articoli, scarico magazzino	T01 DATI COMUNI
Ufficio Prodotti del Traffico	Distribuzione biglietti a Rivendite e pubblico, emissione di abbonamenti, emissione notifiche per multe, incasso multe	T05 DATI COMUNI T08 DATI COMUNI

5. Analisi dei rischi che incombono sui dati (Regola 19.3)

Di seguito vengono riportati i principali rischi per la sicurezza dei dati, si valutano le possibili conseguenze e la gravità riguardo al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

In particolare, si può prendere in considerazione la lista esemplificativa dei seguenti rischi:

- 1) rischi derivanti dai comportamenti degli operatori:
 - sottrazione di credenziali di autenticazione
 - carenza di consapevolezza, disattenzione o incuria
 - comportamenti sleali o fraudolenti
 - errore materiale
- 2) rischi relativi agli strumenti:
 - azione di virus informatici o di programmi suscettibili di recare danno
 - spamming o tecniche di sabotaggio
 - malfunzionamento, indisponibilità o degrado degli strumenti
 - accessi esterni non autorizzati
 - intercettazione di informazioni in rete
- 3) rischi relativi al contesto fisico-ambientale:
 - ingressi non autorizzati a locali/aree ad accesso ristretto
 - sottrazione di strumenti contenenti dati
 - eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi,
 - accidentali o dovuti ad incuria
 - guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
 - errori umani nella gestione della sicurezza fisica

Le tabelle riassuntive che seguono identificano rispecchiano le tre classi omogenee di rischio identificate come sopra e si compongono dei seguenti campi:

- *Codice Rischio*: indica il codice identificativo del rischio
- *Rischio*: indica la minaccia che affligge un trattamento
- *Trattamento*: indica attraverso il codice e la descrizione il trattamento affetto dal relativo rischio.
- *Conseguenze*: descrizione delle principali conseguenze da evitare individuate in relazione ad ogni rischio
- *Danno*: valutazione della dannosità stimata del rischio qualora accadesse, in scala da 1 a 5 (1=minimo, 5 = massimo)
- *Probabilità*: stima della probabilità che un rischio si verifichi, in scala da 1 a 5 (1=minimo, 5 = massimo).
- *Coefficiente rischio*: indicatore omogeneo per la valutazione complessiva del rischio, ottenuto dalla moltiplicazione tra i fattori "Danno" e "Probabilità".

Codice	Rischi associati al comportamento degli operatori	Trattamento	Conseguenze	Danno	Prob.	Coeff. rischio
R001.T01	(O) Sottrazione di credenziali di autenticazione	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R002.T01	(O) Carenza di consapevolezza, disattenzione o incuria	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture		1	1	1
R003.T01	(O) Comportamenti sleali o fraudolenti	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture		1	1	1
R004.T01	(O) Errore materiale	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture		1	1	1
R001.T02	(O) Sottrazione di credenziali di autenticazione	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R002.T02	(O) Carenza di consapevolezza, disattenzione o incuria	T02 Finalità amministrativo contabili: Gestione Officina		1	1	1
R003.T02	(O) Comportamenti sleali o fraudolenti	T02 Finalità amministrativo contabili: Gestione Officina		1	1	1
R004.T02	(O) Errore materiale	T02 Finalità amministrativo contabili: Gestione Officina		1	1	1
R001.T03	(O) Sottrazione di credenziali di autenticazione	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale - calcolo e pagamento di retribuzioni ed emolumenti vari	Distruzione o perdita anche accidentale	1	1	1
R002.T03	(O) Carenza di consapevolezza, disattenzione o incuria	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale		1	1	1
R003.T03	(O) Comportamenti sleali o fraudolenti	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale		1	1	1
R004.T03	(O) Errore materiale	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale		1	1	1
R001.T04	(O) Sottrazione di credenziali di autenticazione	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1
R002.T04	(O) Carenza di consapevolezza, disattenzione o incuria	T04 Finalità amministrativo contabili: Rilevazione Presenze		1	1	1
R003.T04	(O) Comportamenti sleali o fraudolenti	T04 Finalità amministrativo contabili: Rilevazione Presenze		1	1	1
R004.T04	(O) Errore materiale	T04 Finalità amministrativo contabili: Rilevazione Presenze		1	1	1
R001.T05	(O) Sottrazione di credenziali di autenticazione	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1
R002.T05	(O) Carenza di consapevolezza, disattenzione o incuria	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)		1	1	1
R003.T05	(O) Comportamenti sleali o fraudolenti	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)		1	1	1
R004.T05	(O) Errore materiale	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)		1	1	1
R001.T06	(O) Sottrazione di credenziali di autenticazione	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1

R002.T06	(O) Carenza di consapevolezza, disattenzione o incuria	T06 Finalità amministrativo contabili: Archivio dipendenti		1	1	1
R003.T06	(O) Comportamenti sleali o fraudolenti	T06 Finalità amministrativo contabili: Archivio dipendenti		1	1	1
R004.T06	(O) Errore materiale	T06 Finalità amministrativo contabili: Archivio dipendenti		1	1	1
R001.T07	(O) Sottrazione di credenziali di autenticazione	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R002.T07	(O) Carenza di consapevolezza, disattenzione o incuria	T07 Finalità amministrativo contabili: Archivio Sinistri		1	1	1
R003.T07	(O) Comportamenti sleali o fraudolenti	T07 Finalità amministrativo contabili: Archivio Sinistri		1	1	1
R004.T07	(O) Errore materiale	T07 Finalità amministrativo contabili: Archivio Sinistri		1	1	1
R001.T08	(O) Sottrazione di credenziali di autenticazione	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R002.T08	(O) Carenza di consapevolezza, disattenzione o incuria	T08 Finalità amministrativo contabili: Multe		1	1	1
R003.T08	(O) Comportamenti sleali o fraudolenti	T08 Finalità amministrativo contabili: Multe		1	1	1
R004.T08	(O) Errore materiale	T08 Finalità amministrativo contabili: Multe		1	1	1
R001.T09	(O) Sottrazione di credenziali di autenticazione	T09 Finalità amministrativo contabili: Movimento	Distruzione o perdita anche accidentale	1	1	1
R002.T09	(O) Carenza di consapevolezza, disattenzione o incuria	T09 Finalità amministrativo contabili: Movimento		1	1	1
R003.T09	(O) Comportamenti sleali o fraudolenti	T09 Finalità amministrativo contabili: Movimento		1	1	1
R004.T09	(O) Errore materiale	T09 Finalità amministrativo contabili: Movimento		1	1	1
R001.T10	(O) Sottrazione di credenziali di autenticazione	T10 Finalità amministrativo contabili: Concorso autisti	Distruzione o perdita anche accidentale	1	1	1
R002.T10	(O) Carenza di consapevolezza, disattenzione o incuria	T10 Finalità amministrativo contabili: Concorso autisti		1	1	1
R003.T10	(O) Comportamenti sleali o fraudolenti	T10 Finalità amministrativo contabili: Concorso autisti		1	1	1
R004.T10	(O) Errore materiale	T10 Finalità amministrativo contabili: Concorso autisti		1	1	1

Codice	Rischi associati all'uso degli strumenti	Trattamento	Conseguenze	Danno	Prob.	Coeff. rischio
R005.T01	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R006.T01	(S) Spamming o tecniche di sabotaggio	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R007.T01	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R008.T01	(S) Accessi esterni non autorizzati	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Accesso non autorizzato	1	1	1
R009.T01	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T02	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R006.T02	(S) Spamming o tecniche di sabotaggio	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R007.T02	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R008.T02	(S) Accessi esterni non autorizzati	T02 Finalità amministrativo contabili: Gestione Officina	Accesso non autorizzato	1	1	1
R009.T02	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T03	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale - calcolo e pagamento di retribuzioni ed emolumenti vari	Distruzione o perdita anche accidentale	1	1	1
R006.T03	(S) Spamming o tecniche di sabotaggio	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale	Distruzione o perdita anche accidentale	1	1	1
R007.T03	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale	Distruzione o perdita anche accidentale	1	1	1
R008.T03	(S) Accessi esterni non autorizzati	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale	Accesso non autorizzato	1	1	1
R009.T03	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T04	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1
R006.T04	(S) Spamming o tecniche di sabotaggio	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1
R007.T04	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1
R008.T04	(S) Accessi esterni non autorizzati	T04 Finalità amministrativo contabili: Rilevazione Presenze	Accesso non autorizzato	1	1	1
R009.T04	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T05	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1

R006.T05	(S) Spamming o tecniche di sabotaggio	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1
R007.T05	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1
R008.T05	(S) Accessi esterni non autorizzati	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Accesso non autorizzato	1	1	1
R009.T05	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T06	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1
R006.T06	(S) Spamming o tecniche di sabotaggio	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1
R007.T06	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1
R008.T06	(S) Accessi esterni non autorizzati	T06 Finalità amministrativo contabili: Archivio dipendenti	Accesso non autorizzato	1	1	1
R009.T06	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T07	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R006.T07	(S) Spamming o tecniche di sabotaggio	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R007.T07	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T07 Finalità amministrativo contabili: Archivio Sinistri	Accesso non autorizzato	1	1	1
R008.T07	(S) Accessi esterni non autorizzati	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R009.T07	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T08	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R006.T08	(S) Spamming o tecniche di sabotaggio	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R007.T08	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R008.T08	(S) Accessi esterni non autorizzati	T08 Finalità amministrativo contabili: Multe	Accesso non autorizzato	1	1	1
R009.T08	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T09	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T09 Finalità amministrativo contabili: Movimento	Distruzione o perdita anche accidentale	1	1	1
R006.T09	(S) Spamming o tecniche di sabotaggio	T09 Finalità amministrativo contabili: Movimento	Distruzione o perdita anche accidentale	1	1	1
R007.T09	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T09 Finalità amministrativo contabili: Movimento	Distruzione o perdita anche accidentale	1	1	1

R008.T09	(S) Accessi esterni non autorizzati	T09 Finalità amministrativo contabili: Movimento	Accesso non autorizzato	1	1	1
R009.T09	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1
R005.T10	(S) Azione di virus informatici o di programmi suscettibili di recare danno	T10 Finalità amministrativo contabili: Concorso autisti	Distruzione o perdita anche accidentale	1	1	1
R006.T10	(S) Spamming o tecniche di sabotaggio	T10 Finalità amministrativo contabili: Concorso autisti	Distruzione o perdita anche accidentale	1	1	1
R007.T10	(S) Malfunzionamento, indisponibilità o degrado degli strumenti	T10 Finalità amministrativo contabili: Concorso autisti	Distruzione o perdita anche accidentale	1	1	1
R008.T10	(S) Accessi esterni non autorizzati	T10 Finalità amministrativo contabili: Concorso autisti	Accesso non autorizzato	1	1	1
R009.T10	(S) Intercettazione di informazioni in rete		Distruzione o perdita anche accidentale	1	1	1

Codice	Rischi associati al contesto fisico ed ambientale	Trattamento	Conseguenze	Danno	Prob.	Coeff. rischio
R010.T01	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Accesso non autorizzato	1	1	1
R011.T01	(C) Sottrazione di documenti contenenti dati	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R012.T01	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R013.T01	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R014.T01	(C) Errori umani nella gestione della sicurezza fisica	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture	Distruzione o perdita anche accidentale	1	1	1
R010.T02	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T02 Finalità amministrativo contabili: Gestione Officina	Accesso non autorizzato	1	1	1
R011.T02	(C) Sottrazione di documenti contenenti dati	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R012.T02	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R013.T02	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R014.T02	(C) Errori umani nella gestione della sicurezza fisica	T02 Finalità amministrativo contabili: Gestione Officina	Distruzione o perdita anche accidentale	1	1	1
R010.T03	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale - calcolo e pagamento di retribuzioni ed emolumenti vari	Accesso non autorizzato	1	1	1
R011.T03	(C) Sottrazione di documenti contenenti dati	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale	Distruzione o perdita anche accidentale	1	1	1
R012.T03	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale	Distruzione o perdita anche accidentale	1	1	1
R013.T03	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale	Distruzione o perdita anche accidentale	1	1	1
R014.T03	(C) Errori umani nella gestione della sicurezza fisica	T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale	Distruzione o perdita anche accidentale	1	1	1
R010.T04	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T04 Finalità amministrativo contabili: Rilevazione Presenze	Accesso non autorizzato	1	1	1
R011.T04	(C) Sottrazione di documenti contenenti dati	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1
R012.T04	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1
R013.T04	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1
R014.T04	(C) Errori umani nella gestione della sicurezza fisica	T04 Finalità amministrativo contabili: Rilevazione Presenze	Distruzione o perdita anche accidentale	1	1	1

R010.T05	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Accesso non autorizzato	1	1	1
R011.T05	(C) Sottrazione di documenti contenenti dati	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1
R012.T05	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1
R013.T05	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1
R014.T05	(C) Errori umani nella gestione della sicurezza fisica	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Distruzione o perdita anche accidentale	1	1	1
R010.T06	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T06 Finalità amministrativo contabili: Archivio dipendenti	Accesso non autorizzato	1	1	1
R011.T06	(C) Sottrazione di documenti contenenti dati	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1
R012.T06	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1
R013.T06	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1
R014.T06	(C) Errori umani nella gestione della sicurezza fisica	T06 Finalità amministrativo contabili: Archivio dipendenti	Distruzione o perdita anche accidentale	1	1	1
R010.T07	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T07 Finalità amministrativo contabili: Archivio Sinistri	Accesso non autorizzato	1	1	1
R011.T07	(C) Sottrazione di documenti contenenti dati	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R012.T07	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R013.T07	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R014.T07	(C) Errori umani nella gestione della sicurezza fisica	T07 Finalità amministrativo contabili: Archivio Sinistri	Distruzione o perdita anche accidentale	1	1	1
R010.T08	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T08 Finalità amministrativo contabili: Multe	Accesso non autorizzato	1	1	1
R011.T08	(C) Sottrazione di documenti contenenti dati	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R012.T08	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R013.T08	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R014.T08	(C) Errori umani nella gestione della sicurezza fisica	T08 Finalità amministrativo contabili: Multe	Distruzione o perdita anche accidentale	1	1	1
R010.T09	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T09 Finalità amministrativo contabili: Movimento	Accesso non autorizzato	1	1	1
R011.T09	(C) Sottrazione di documenti contenenti dati	T09 Finalità amministrativo contabili: Movimento	Distruzione o perdita anche accidentale	1	1	1

R012.T09	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T09 Finalità Movimento	amministrativo	contabili: Distruzione o perdita anche accidentale	1	1	1
R013.T09	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T09 Finalità Movimento	amministrativo	contabili: Distruzione o perdita anche accidentale	1	1	1
R014.T09	(C) Errori umani nella gestione della sicurezza fisica	T09 Finalità Movimento	amministrativo	contabili: Distruzione o perdita anche accidentale	1	1	1
R010.T10	(C) Ingressi non autorizzati a locali/aree ad accesso ristretto	T10 Finalità Concorso autisti	amministrativo	contabili: Accesso non autorizzato	1	1	1
R011.T10	(C) Sottrazione di documenti contenenti dati	T10 Finalità Concorso autisti	amministrativo	contabili: Distruzione o perdita anche accidentale	1	1	1
R012.T10	(C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dovuti a incuria	T10 Finalità Concorso autisti	amministrativo	contabili: Distruzione o perdita anche accidentale	1	1	1
R013.T10	(C) Guasti a sistemi complementari (impianto elettrico, climatizzazione...)	T10 Finalità Concorso autisti	amministrativo	contabili: Distruzione o perdita anche accidentale	1	1	1
R014.T10	(C) Errori umani nella gestione della sicurezza fisica	T10 Finalità Concorso autisti	amministrativo	contabili: Distruzione o perdita anche accidentale	1	1	1

Strumenti impiegati nel trattamento

Sono stati individuati come sorgenti soggette a rischio le seguenti categorie di strumenti utilizzati per il trattamento:

Strumenti	Legenda
Schedari e altri supporti cartacei custoditi nell'area controllata	A
Elaboratori non in rete custoditi nell'area controllata	B
Elaboratori in rete privata custoditi nell'area controllata	C
Elaboratori in rete pubblica	D

Fattori di rischio	Basso	Medio	Elevato
Rischio d'area legato all'accesso non autorizzato nei locali			A B C D
Rischio guasti tecnici hardware, software, supporti		C D	B
Rischio penetrazione nelle reti di comunicazione			D
Rischio legato ad errori umani	A	B	C D
Rischio d'area per possibili eventi distruttivi			A B C D

6. Misure da adottare ed in essere (Regola 19.4)

In questa sezione si riportano le misure in essere e da adottare per contrastare ognuno dei rischi individuati nel precedente paragrafo. Per misura s'intende lo specifico intervento tecnico ovvero organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia.

Le misure così individuate, tengono conto dei seguenti fondamentali aspetti: protezione delle aree e dei locali; archiviazione e custodia di atti documenti e supporti contenenti dati personali ed infine misure logiche di sicurezza.

- **Codice Misura:** individua il codice univoco associato alla misura
- **Misura:** descrive sinteticamente la misura idonea a ridurre al minimo i rischi individuati
- **Rischio:** indica il codice e la descrizione del rischio che si intende contrastare
- **Trattamento:** indica il codice e la descrizione del trattamento interessato
- **Ambito:** specifica l'ambito d'adozione della misura quale "fisico", "logico", "organizzativo" ovvero "minima" se prevista dal disciplinare tecnico.
- **Tipo Misura:** indica la natura della misura scelta tra le evenienze di "prevenzione", di "contrasto", e di "contenimento degli effetti".
- **Stato:** "in essere" o "da adottare"
- **Scadenza Adozione:** è la data di prevista adozione entro la quale il Titolare intende adottare la misura descritta.
- **Unità Operativa:** indica l'unità operativa preposta all'adozione della misura indicata.

Codice	Misura	Rischio	Trattamento	Ambito	Tipo di misura	Stato	Scadenza adozione	Unità Operativa
M001.T01	Dominio NT	R001.T01 – (O) Sottrazione di credenziali di autenticazione	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fat-ture	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Ragioneria e Magazzino
M005.T01	Antivirus sulle singole postazioni	R005.T01 – (S) Azione di virus informatici o di programmi suscettibili di recare danno	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fat-ture	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Ragioneria e Magazzino
M008.T01	Firewall (n. 2): Router e PC con S.O. Win98/2000/XP con in più la funzione di NAT	R008.T01 – (S) Accessi esterni non autorizzati	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fat-ture	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Ragioneria e Magazzino
M010.T01	Sistemi di allarme interni? Più di uno?	R010.T01 – (C) Ingressi non autorizzati a locali / aree ad accesso ristretto	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fat-ture	Fisico	Prevenzione	Da adottare	?	Ufficio Ragioneria e Magazzino
M012.T01	Dispositivo antincendio presente con segnale di allarme sia acustico che visivo	R012.T01 . (C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dotti a incuria	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fat-ture	Fisico	Prevenzione	Da adottare	?	Ufficio Ragioneria e Magazzino
M001.T02	Dominio NT	R001.T02 – (O) Sottrazione di credenziali di autenticazione	T02 Finalità amministrativo contabili: Gestione Officina	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Tecnico
M005.T02	Antivirus sulle singole postazioni	R005.T02 – (S) Azione di virus informatici o di programmi suscettibili di recare danno	T02 Finalità amministrativo contabili: Gestione Officina	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Tecnico

M008.T02	Firewall (n. 2): Router (Cisco) e PC con S.O. Win98/2000/XP con in più la fun- zione di NAT	R008.T02 - (S) Accessi esterni non autorizzati	T02 Finalità ammini- strativo contabili: Gestione Officina	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Tec- nico
M010.T02	Sistemi di allarme interni? Più di uno?	R010.T02 - (C) Ingressi non au- torizzati a locali / aree ad accesso ristretto	T02 Finalità ammini- strativo contabili: Gestione Officina	Fisico	Prevenzione	Da adot- tare	?	Ufficio Tec- nico
M012.T02	Dispositivo antin- cendio presente con segnale di al- larne sia acustico che visivo	R012.T02 . (C) Eventi distruttivi, naturali o artifi- ciali; dolosi, acci- dentali o dotti a incuria	T02 Finalità ammini- strativo contabili: Gestione Officina	Fisico	Prevenzione	Da adot- tare	?	Ufficio Tec- nico
M001.T03	Dominio NT	R001.T03 - (O) Sottrazione di credenziali autenticazione	T03 Finalità ammini- strativo contabili: Trattamento giuridi- co ed economico del personale - calcolo e pagamento di retri- buzioni ed emolu- menti vari	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Re- tribuzioni
M005.T03	Antivirus sulle sin- gole postazioni	R005.T03 - (S) Azione di virus informatici o di programmi su- scettibili di recare danno	T03 Finalità ammini- strativo contabili: Trattamento giuridi- co ed economico del personale	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Re- tribuzioni
M008.T03	Firewall (n. 2): Router e PC con S.O. Win98/2000/XP con in più la fun- zione di NAT	R008.T03 - (S) Accessi esterni non autorizzati	T03 Finalità ammini- strativo contabili: Trattamento giuridi- co ed economico del personale	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Re- tribuzioni
M010.T03	Sistemi di allarme interni? Più di uno?	R010.T03 - (C) Ingressi non au- torizzati a locali / aree ad accesso ristretto	T03 Finalità ammini- strativo contabili: Trattamento giuridi- co ed economico del personale	Fisico	Prevenzione	Da adot- tare	?	Ufficio Re- tribuzioni
M012.T03	Dispositivo antin- cendio presente con segnale di al- larne sia acustico che visivo	R012.T03 . (C) Eventi distruttivi, naturali o artifi- ciali; dolosi, acci- dentali o dotti a incuria	T03 Finalità ammini- strativo contabili: Trattamento giuridi- co ed economico del personale	Fisico	Prevenzione	Da adot- tare	?	Ufficio Re- tribuzioni
M001.T04	Dominio NT	R001.T04 - (O) Sottrazione di credenziali autenticazione	T04 Finalità ammini- strativo contabili: Rilevazione Presen- ze	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Re- tribuzioni
M005.T04	Antivirus	R005.T04 - (S) Azione di virus informatici o di programmi su- scettibili di recare danno	T04 Finalità ammini- strativo contabili: Rilevazione Presen- ze	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Re- tribuzioni
M008.T04	Firewall (n. 2): Router e PC con S.O. Win2000/XP con in più la fun- zione di NAT	R008.T04 - (S) Accessi esterni non autorizzati	T04 Finalità ammini- strativo contabili: Rilevazione Presen- ze	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Re- tribuzioni
M010.T04	Sistemi di allarme interni? Più di uno?	R010.T04 - (C) Ingressi non au- torizzati a locali / aree ad accesso ristretto	T04 Finalità ammini- strativo contabili: Rilevazione Presen- ze	Fisico	Prevenzione	Da adot- tare	?	Ufficio Re- tribuzioni

M012.T04	Dispositivo antincendio presente con segnale di allarme sia acustico che visivo	R012.T04 - (C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dotti a incuria	T04 Finalità amministrativo contabili: Rilevazione Presenze	Fisico	Prevenzione	Da adottare	?	Ufficio Retribuzioni
M001.T05	Dominio NT	R001.T05 - (O) Sottrazione di credenziali di autenticazione	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Prodotti del Traffico
M005.T05	Antivirus sulle singole postazioni	R005.T05 - (S) Azione di virus informatici o di programmi suscettibili di recare danno	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Prodotti del Traffico
M008.T05	Firewall (n. 1): Router e PC con S.O. Win98/2000/XP con in più la funzione di NAT	R008.T05 - (S) Accessi esterni non autorizzati	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Prodotti del Traffico
M010.T05	Sistemi di allarme interno	R010.T05 - (C) Ingressi non autorizzati a locali / aree ad accesso ristretto	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Fisico	Prevenzione	In essere		Ufficio Prodotti del Traffico
M012.T05	Dispositivo antincendio presente con segnale di allarme sia acustico che visivo	R012.T05 - (C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dotti a incuria	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti)	Fisico	Prevenzione	In essere		Ufficio Prodotti del Traffico
M001.T06	Dominio NT	R001.T06 - (O) Sottrazione di credenziali di autenticazione	T06 Finalità amministrativo contabili: Archivio dipendenti	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Retribuzioni
M005.T06	Antivirus sulle singole postazioni	R005.T06 - (S) Azione di virus informatici o di programmi suscettibili di recare danno	T06 Finalità amministrativo contabili: Archivio dipendenti	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Retribuzioni
M008.T06	Firewall (n. 2): Router (Cisco) e PC con S.O. Win98/2000/XP con in più la funzione di NAT	R008.T06 - (S) Accessi esterni non autorizzati	T06 Finalità amministrativo contabili: Archivio dipendenti	Minima - "Allegato B"	Prevenzione	In essere		Ufficio Retribuzioni
M010.T06	Sistemi di allarme interni? Più di uno?	R010.T06 - (C) Ingressi non autorizzati a locali / aree ad accesso ristretto	T06 Finalità amministrativo contabili: Archivio dipendenti	Fisico	Prevenzione	Da adottare	?	Ufficio Retribuzioni
M012.T06	Dispositivo antincendio presente con segnale di allarme sia acustico che visivo	R012.T06 - (C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dotti a incuria	T06 Finalità amministrativo contabili: Archivio dipendenti	Fisico	Prevenzione	Da adottare	?	Ufficio Retribuzioni

M001.T07	Dominio NT	R001.T07 - (O) Sottrazione di credenziali di autenticazione	T07 Finalità amministrativo contabili: Archivio Sinistri	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Sinistri
M005.T07	Antivirus sulle singole postazioni	R005.T07 - (S) Azione di virus informatici o di programmi suscettibili di recare danno	T07 Finalità amministrativo contabili: Archivio Sinistri	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Sinistri
M008.T07	Firewall (n. 2): Router e PC con S.O. Win98/2000/XP con in più la funzione di NAT	R008.T07 - (S) Accessi esterni non autorizzati	T07 Finalità amministrativo contabili: Archivio Sinistri	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Sinistri
M010.T07	Sistemi di allarme interni? Più di uno?	R010.T07 - (C) Ingressi non autorizzati a locali / aree ad accesso ristretto	T07 Finalità amministrativo contabili: Archivio Sinistri	Fisico	Prevenzione	Da adottare	?		Ufficio Sinistri
M012.T07	Dispositivo antincendio presente con segnale di allarme sia acustico che visivo	R012.T07 - (C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dotti a incuria	T07 Finalità amministrativo contabili: Archivio Sinistri	Fisico	Prevenzione	Da adottare	?		Ufficio Sinistri
M001.T08	Dominio NT	R001.T08 - (O) Sottrazione di credenziali di autenticazione	T08 Finalità amministrativo contabili: Multe	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Prodotti del Traffico
M005.T08	Antivirus sulle singole postazioni	R005.T08 - (S) Azione di virus informatici o di programmi suscettibili di recare danno	T08 Finalità amministrativo contabili: Multe	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Prodotti del Traffico
M008.T08	Firewall (n. 1): Router e PC con S.O. Win95/Win98/2000/XP con in più la funzione di NAT	R008.T08 - (S) Accessi esterni non autorizzati	T08 Finalità amministrativo contabili: Multe	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Prodotti del Traffico
M010.T08	Sistemi di allarme interno	R010.T08 - (C) Ingressi non autorizzati a locali / aree ad accesso ristretto	T08 Finalità amministrativo contabili: Multe	Fisico	Prevenzione	In essere			Ufficio Prodotti del Traffico
M012.T08	Dispositivo antincendio presente con segnale di allarme sia acustico che visivo	R012.T01 - (C) Eventi distruttivi, naturali o artificiali; dolosi, accidentali o dotti a incuria	T08 Finalità amministrativo contabili: Multe	Fisico	Prevenzione	In essere			Ufficio Prodotti del Traffico
M001.T09	Dominio NT	R001.T09 - (O) Sottrazione di credenziali di autenticazione	T09 Finalità amministrativo contabili: Movimento	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Programmi e Turni - Addetti Movimento
M005.T09	Antivirus sulle singole postazioni	R005.T09 - (S) Azione di virus informatici o di programmi suscettibili di recare danno	T09 Finalità amministrativo contabili: Movimento	Minima - "Allegato B"	Prevenzione	In essere			Ufficio Programmi e Turni - Addetti Movimento

M008.T09	Firewall (n. 2): Router (Cisco) e PC con S.O. Win98/2000/XP con in più la fun- zione di NAT	R008.T09 – (S) Accessi esterni non autorizzati	T09 Finalità ammini- strativo contabili: Movimento	Minima - “Allegato B”	Prevenzione	In essere		Ufficio Pro- grammi e Turni – Ad- detti Movi- mento
M010.T09	Sistemi di allarme interni? Più di uno?	R010.T09 – (C) Ingressi non au- torizzati a locali / aree ad accesso ristretto	T09 Finalità ammini- strativo contabili: Movimento	Fisico	Prevenzione	Da adot- tare	?	Ufficio Pro- grammi e Turni – Ad- detti Movi- mento
M012.T09	Dispositivo antin- cendio presente con segnale di al- larne sia acustico che visivo	R012.T09 . (C) Eventi distruttivi, naturali o artifi- ciali; dolosi, acci- dentali o dotti a incuria	T09 Finalità ammini- strativo contabili: Movimento	Fisico	Prevenzione	Da adot- tare	?	Ufficio Pro- grammi e Turni – Ad- detti Movi- mento
M001.T10	Dominio NT	R001.T10 – (O) Sottrazione di credenziali di autenticazione	T10 Finalità ammini- strativo contabili: Concorso autisti	Minima - “Allegato B”	Prevenzione	In essere		Ufficio Se- greteria
M005.T10	Antivirus sulle sin- gole postazioni	R005.T10 – (S) Azione di virus informatici o di programmi su- scettibili di recare danno	T10 Finalità ammini- strativo contabili: Concorso autisti	Minima - “Allegato B”	Prevenzione	In essere		Ufficio Se- greteria
M008.T10	Firewall (n. 1): Router e PC con S.O. Win98/2000/XP con in più la fun- zione di NAT	R008.T10 – (S) Accessi esterni non autorizzati	T10 Finalità ammini- strativo contabili: Concorso autisti	Minima - “Allegato B”	Prevenzione	In essere		Ufficio Se- greteria
M010.T10	Sistemi di allarme interni? Più di uno?	R010.T10 – (C) Ingressi non au- torizzati a locali / aree ad accesso ristretto	T10 Finalità ammini- strativo contabili: Concorso autisti	Fisico	Prevenzione	Da adot- tare	?	Ufficio Se- greteria
M012.T10	Dispositivo antin- cendio presente con segnale di al- larne sia acustico che visivo	R012.T10 . (C) Eventi distruttivi, naturali o artifi- ciali; dolosi, acci- dentali o dotti a incuria	T10 Finalità ammini- strativo contabili: Concorso autisti	Fisico	Prevenzione	Da adot- tare	?	Ufficio Se- greteria

6.1 Controllo generale sullo stato della sicurezza.

Al responsabile per la sicurezza è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

A tale fine, è previsto che al responsabile venga affidato un budget annuo di euro....., che può utilizzare in autonomia, a condizione che il singolo investimento non superi l'importo di euro..... per singoli investimenti, che superino l'importo di euro....., il responsabile dovrà ottenere l'autorizzazione di.....

Ogni.....mesi è prevista una riunione del responsabile per la sicurezza con i membri del Consiglio di Amministrazione, durante la quale il responsabile renderà conto delle somme spese e, se la situazione lo richiede, si provvederà eventualmente ad aumentare il budget annuo di spese.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile per la sicurezza e le persone da questo appositamente incaricate provvedono con frequenza settimanale / mensile, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette
- verificare l'integrità dei dati e delle loro copie di backup
- verificare la sicurezza delle trasmissioni in rete
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

Dell'attività di verifica svolta viene redatto un verbale, che viene conservato dal Titolare (eventualmente: e allegato al Documento programmatico sulla sicurezza).

Periodicamente, con frequenza.....(generalmente annuale, ma a volte semestrale, o addirittura trimestrale per le organizzazioni più complesse), ci si rivolge ad una società specializzata, che effettua l'audit di sicurezza: con tale termine si intende l'attività di verifica, che potrà avvenire in modo estemporaneo, anche con verifiche casuali e non annunciate.

Obiettivo dell'audit di sicurezza è di verificare che tutte le misure implementate, sia quelle tecnologiche che quelle organizzative, svolgano correttamente le funzionalità per cui sono state adottate.

7. Criteri e modalità di ripristino della disponibilità dei dati (Regola 19.5)

In questa sezione sono descritti i criteri e le procedure adottati per il salvataggio ed il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo, pertanto è essenziale che quando siano necessarie, le copie dei dati anche cartacei siano disponibili e le procedure di reinstallazione siano efficaci.

E' in prima istanza il disciplinare tecnico a dettare le misure minime da adottare, in tutti i casi bisogna procedere al solo salvataggio dei dati almeno settimanalmente, nei casi di trattamento di dati sensibili e/o giudiziari esiste l'obbligo del loro ripristino entro e non oltre sette giorni.

Per quanto riguarda il ripristino ed il salvataggio, le informazioni essenziali sono:

- **Criteri e procedure:** descrive sinteticamente le procedure ed i criteri individuati per il salvataggio ed il ripristino dei dati
- **Trattamenti coinvolti :** indica i codici e le descrizioni dei trattamenti coinvolti
- **Banca dati :** è la base di dati interessata dalla procedura
- **Frequenza delle prove di ripristino:** indicazione dei tempi previsti per effettuare i test di efficacia delle procedure di salvataggio/ripristino dei dati adottate
- **Data della prossima prova di ripristino:** è indicata la data del prossimo test di efficacia
- **Luoghi di custodia dei supporti:** contiene l'indicazione di quali sono i locali dove sono custoditi e copie o dove avviene il ripristino.
- **Incaricati al Backup:** contiene i nomi delle persone cui è affidato il compito di eseguire il backup
- **Incaricati al Ripristino:** contiene i nomi dei soggetti a cui è affidata l'operazione di ripristino.

Criteri e procedure	Trattamenti coinvolti	Banche dati	Frequenza	Prossima prova di ripristino	Luoghi di custodia dei supporti	Incaricato Backup	Incaricato ripristino
Backup dati su nastro magnetico	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture T02 Finalità amministrativo contabili: Gestione Officina T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale - calcolo e pagamento di retribuzioni ed emolumenti vari T04 Finalità amministrativo contabili: Rilevazione Presenze T06 Finalità amministrativo contabili: Archivio dipendenti T07 Finalità amministrativo contabili: Archivio Sinistri T09 Finalità amministrativo contabili: Movimento T10 Finalità amministrativo contabili: Concorso autisti	Database	Giornaliera	N/A	Cassaforte ignifuga in vano realizzato nel sottoscala palazzina amministrazione e chiuso con porta in alluminio con serratura	Area Informatica	Area Informatica
Backup su CD	T05 Finalità amministrativo contabili: Gestione degli Introiti derivanti dalla vendita di titoli di viaggio (biglietti ed abbonamenti) T08 Finalità amministrativo contabili: Multe	Database	Giornaliera	N/A	Armadio con serratura	Ufficio Prodotti del Traffico	Area Informatica
Backup su CD	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture T02 Finalità amministrativo contabili: Gestione Officina T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale - calcolo e pagamento di retribuzioni ed emolumenti vari T04 Finalità amministrativo contabili: Rilevazione Presenze	Database	Settimanale	Settimanale	Cassaforte ignifuga in vano realizzato nel sottoscala palazzina amministrazione e chiuso con porta in alluminio con serratura	Area Informatica	Area Informatica

Backup su PC Capo Area Informatica	T06 Finalità amministrativo contabili: Archivio dipendenti T07 Finalità amministrativo contabili: Archivio Sinistri T09 Finalità amministrativo contabili: Movimento T10 Finalità amministrativo contabili: Concorso autisti	Database	Settimanale	N/A		Area Informatica	Area Informatica
Backup incrociato tra 2 Server	T01 Finalità amministrativo contabili: Gestione Clienti, Fornitori, Ordini, Fatture T02 Finalità amministrativo contabili: Gestione Officina T03 Finalità amministrativo contabili: Trattamento giuridico ed economico del personale - calcolo e pagamento di retribuzioni ed emolumenti vari T04 Finalità amministrativo contabili: Rilevazione Presenze T06 Finalità amministrativo contabili: Archivio dipendenti T07 Finalità amministrativo contabili: Archivio Sinistri T09 Finalità amministrativo contabili: Movimento T10 Finalità amministrativo contabili: Concorso autisti	Database	Settimanale	N/A		Area Informatica	Area Informatica

7.1 Scheda descrittiva delle misure adottate.

Scheda nr.	01	Compilata da	Dott. Ciro Russo	Data di compilazione	14/06/2004
Misura	Backup dati su supporto magnetico				
Descrizione sintetica	Il backup è programmato da software per essere eseguito giornalmente, dopo le ore 23.00, previo backup del database su cartella dati PlusSqlBack				
Elementi descrittivi					
Data di aggiornamento: 14/06/2004					

Scheda nr.	02	Compilata da	Dott. Ciro Russo	Data di compilazione	14/06/2004
Misura	Backup dati su supporto magnetico				
Descrizione sintetica	Il backup è programmato da software per essere eseguito giornalmente, dopo le ore 23.00				
Elementi descrittivi					
Data di aggiornamento: 14/06/2004					

Scheda nr.	03	Compilata da	Dott. Ciro Russo	Data di compilazione	14/06/2004
Misura	Backup dati su PC Capo Area Informatica				
Descrizione sintetica	Viene effettuata giornalmente una copia compressa (in formato ZIP) degli archivi interessati; viene quindi testata l'integrità dell'archivio compresso.				
Elementi descrittivi					
Data di aggiornamento: 14/06/2004					

Scheda nr.	04	Compilata da	Dott. Ciro Russo	Data di compilazione	14/06/2004
Misura	Backup dati su PC Capo Area Informatica				
Descrizione sintetica	Viene effettuata giornalmente una copia integrale degli archivi interessati.				
Elementi descrittivi					
Data di aggiornamento: 14/06/2004					

Scheda nr.	05	Compilata da	Dott. Ciro Russo	Data di compilazione	14/06/2004
Misura	Backup dati su CD				
Descrizione sintetica	Viene effettuata settimanalmente una copia degli archivi interessati, il CD generato viene sottoposto a verifica dei dati contenuti con quelli di origine e quindi viene testata l'integrità dell'archivio compresso.				
Elementi descrittivi					
Data di aggiornamento: 14/06/2004					

7.2 La protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, i locali ove si svolge il trattamento dei dati sono protetti da:

- dispositivi antincendio previsti dalla normativa vigente
- gruppo di continuità dell'alimentazione elettrica
- impianto di condizionamento

Sono adottate le seguenti misure per impedire accessi non autorizzati (elencare):

- l'accesso all'Azienda da parte di persone non appartenenti all'Azienda è consentito previa presentazione di un documento d'identità al servizio di vigilanza posto all'ingresso dell'Azienda ed autorizzazione da parte dell'ufficio di destinazione; inoltre l'accesso agli uffici dell'amministrazione è consentito tramite portoncino in anticorodal, dotato di serratura elettrica, comandata da personale aziendale adibito al controllo degli accessi con le modalità stabilite dall'Ordine di Servizio n. **XXXX** del **XXXXXXXXXXXX**
- l'accesso ad aree ristrette (locali server) è consentito solo ai responsabili della manutenzione ed al personale dell'Area Informatica; una copia della chiave di accesso è custodita in apposita bacheca nel gabbiotto della vigilanza.

7.3 Custodia e archiviazione dei dati

Agli incaricati sono state impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti. In particolare sono state fornite direttive per:

- il corretto accesso ai dati personali, sensibili e giudiziari;
- la conservazione e la custodia di documenti, atti e supporti contenenti dati personali, sensibili e giuridici;
- la definizione delle persone autorizzate ad accedere ai locali archivio e le modalità di accesso;

7.4 Misure logiche di sicurezza

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure.

- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici
- autorizzazione e definizione delle tipologie di dati ai quali gli incaricati possono accedere e utilizzare al fine delle proprie mansioni lavorative
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.

Accesso ai dati e istruzioni impartite agli incaricati

Gli incaricati al trattamento dei dati, dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password)
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento
- obbligo di assoluta riservatezza
- divieto di divulgazione della password di accesso al sistema

8. Scadenario delle misure da adottare

Per facilitare il compito di coloro che dovranno implementare l'adozione di tutte le misure reputate idonee a ridurre al minimo i rischi e come ulteriore contenuto distintivo si fornisce di seguito lo scadenario delle misure idonee.

- **Data scadenza:** è la data entro e non oltre la quale si è preso l'impegno di adottare la misura
- **Codice Misura:** è il codice che individua univocamente la misura
- **Unità operativa:** è la struttura organizzativa cui spetta il compito di adottare quella misura.

Misura	Data scadenza	Incaricato dell'adozione
Antivirus	In essere	Area Informatica

9. Pianificazione degli interventi formativi (Regola 19.6)

In ottemperanza alla disposizione dell'articolo 34 è previsto l'aggiornamento periodico di quanto individuato attraverso il Mansionario, questo si concretizza in interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implicino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implicino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

In ogni caso, sono previste riunioni periodiche, una volta l'anno, per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.

Per l'anno 2004, è previsto che, mediamente, ogni incaricato dedichi una giornata lavorativa alla formazione in materia di trattamento dei dati personali.

Nella seguente tabella si riassume un quadro sintetico dell'impegno formativo che si prevede di sostenere, nell'anno 2004, in attuazione della normativa privacy:

9.1 Pianificazione degli interventi formativi previsti

Corso	Descrizione sintetica	Unità operative coinvolte	Numero di incaricati interessati	Numero di incaricati già formati/da formare nell'anno	Calendario
F_OCEANO	Istruzione all'uso e custodia delle credenziali di accesso ai dati ed alla riservatezza dei dati trattati	Ragioneria Magazzino Ufficio tecnico Contratti e acquisti	15	15	
F_OFFICINA		Ufficio tecnico Area tecnica	3	3	
F_SISPAC		Retribuzioni	4	4	
F_CARPERS		Ufficio retribuzioni Segreteria	7	7	
F_SINISTRI		Pubbliche relazioni Ufficio sinistri	3	3	
F_MULTA		Ufficio prodotti del traffico Addetti all'inserimento multe	5	5	
F_TURNI		Uffici Movimento Addetti al movimento	25	25	
F_PRESENZE	Istruzione alla procedura di salvataggio dei dati	Retribuzioni/Presenza	3	3	
F_CONCORSO	Riservatezza dei dati trattati	Segreteria	3	3	
Data di aggiornamento: 16/06/2004					

Protezione di strumenti e dati

Premesso che non vengono trattati dati sensibili e giudiziari in rete, il sistema di elaborazione è comunque protetto da programmi antivirus e di sistema firewall antiintrusione. Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione. Agli incaricati è stato affidato il compito di aggiornare periodicamente (precisare la periodicità) il sistema di protezione.

Supporti rimovibili

Anche se le norme prevedono particolari cautele solo per i supporti rimovibili contenenti dati sensibili e giuridici, la tutela per il trattamento viene estesa ai dati personali come segue:

- custodia dei supporti in contenitori chiusi a chiave in locali con accesso ai soli autorizzati
- cancellazione o distruzione del supporto una volta cessate le ragioni per la conservazione

10. Dichiarazioni d'impegno e firma

Il presente documento, redatto nel20XX, viene firmato in calce da:
Enzo Manco, in qualità di rappresentante legale del Titolare.

Il presente Documento programmatico sulla sicurezza verrà sottoposto per l'approvazione al Consiglio di Amministrazione, e successivamente trascritto nel libro sociale che riporta le delibere prese dallo stesso.

L'originale del presente documento viene custodito presso la sede della società, per essere esibito in caso di controlli.

Una sua copia verrà consegnata:

- a ciascun responsabile interno del trattamento dei dati personali
- ai responsabili esterni del trattamento dei dati personali
- a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali (ad esempio, nel caso in cui dovessimo essere nominati responsabili per determinati trattamenti di dati personali).

Nella relazione accompagnatoria del bilancio di esercizio si riferisce dell'avvenuta redazione del presente documento, che costituisce la prima redazione del Documento programmatico sulla sicurezza

Luogo e data.....

Firma del rappresentante legale del Titolare.....

ORGANIGRAMMA PRIVACY

TITOLARE DEI DATI		
A.M.A.T. S.p.A.		
RESPONSABILI	INCARICATI AL TRATTAMENTO	Area/Ufficio
Iervoglioni Francesco		Area Contabilità e Bilancio
	Di Corrado Giuseppe	Ufficio Ragioneria
	Greco Vincenzo	Ufficio Ragioneria
	Angiulli Ettore	Ufficio Ragioneria
	Cardellicchio Giuseppe	Ufficio Ragioneria
Russo Ciro		Area Informatica
Russo Cosimo		Area Segreteria
		Ufficio Segreteria
	Stasolla Lorenzo	Ufficio Segreteria
Menenti Fabiola		Area Personale
	Picchi Enrico	Ufficio Retribuzioni
	Fornaro Vincenzo	Ufficio Retribuzioni
	Cellammare Giovanni	Ufficio Retribuzioni
	Massari Amedeo	Ufficio Retribuzioni
Tursi Tiziana		Unità AA.GG.
Ancarola Bruno		Area Contratti e Acquisti – Magazzino
	Cigliese Cosimo	Ufficio Contratti e Acquisti
	Rota Stefano	Ufficio Contratti e Acquisti
	Conte Roberto	Ufficio Contratti e Acquisti
	Di Taranto Vito	Ufficio Magazzino
	Battista Antonio	Ufficio Magazzino
	Torcello Salvatore	Magazzino distribuzione
	De Vietro Angelo	Magazzino distribuzione
	Semeraro Francesco	Magazzino distribuzione
	Zaccaria Cosimo	Magazzino distribuzione
Rizzo Pietro		Area Tecnica
	Rochira Vincenzo	Ufficio Tecnico
	Paurini Gregorio	Ufficio Tecnico
	Massaro Cosimo	Ufficio Tecnico
Ferrante Giuseppe		Area Movimento
D'addario Giuseppe		Ufficio Programmazione
	Tommaselli Pietro	Ufficio Programmazione
	Stanisci Francesco	Ufficio Programmazione
	Sallustio Raffaele	Ufficio Programmazione
	Rizzo Pietro	Addetti Movimento e Traffico
	Fanelli Francesco	Addetti Movimento e Traffico
	Picuno Luciano	Addetti Movimento e Traffico
	Tommaselli	Addetti Movimento e Traffico
	Cappellano Giuseppe	Addetti Movimento e Traffico
	Lorè Luca	Addetti Movimento e Traffico
	Pignatale Francesco	Addetti Movimento e Traffico
	Mongelli Giuseppe	Addetti Movimento e Traffico
	Troncone Antonio	Addetti Movimento e Traffico
	Laviola Nicola	Addetti Movimento e Traffico
	Mancini Emilio	Addetti Movimento e Traffico
	Sportelli Rosario	Addetti Movimento e Traffico
	Vasco Giovanni	Addetti Movimento e Traffico
Nicola Carrieri		Ufficio Prodotti del Traffico
	Sagliocca Paolo	Ufficio Prodotti del Traffico
	Vecchio Pietro	Ufficio Prodotti del Traffico
	Carrino Giovanni	Ufficio Prodotti del Traffico
	Barbaro Giuseppe	Ufficio Prodotti del Traffico

	Pellicoro Giuseppe	Ufficio Prodotti del Traffico
	Bernardi Donato	Ufficio Prodotti del Traffico
	Santoro Cosimino	Ufficio Prodotti del Traffico

FAC SIMILE

Lettera di incarico al trattamento dei dati

Ai sensi del D.Lgs. 196/2003 con la presente La incarichiamo del trattamento dei dati necessari per la gestione, normativa, contabile e previdenziale, per lo svolgimento dell'attività di gestione paghe e consulenza aziendale e fiscale.

Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua l'ambito del trattamento consentito.

Istruzioni specifiche sul trattamento dei dati

Le rammentiamo quanto disposto dall'art. 11 del D.Lgs. 196/2003 ex art. 9 legge 675/1996 I dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento - in termini compatibili con tali scopi
- esatti e se necessario aggiornati
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati

Inoltre si richiede la Sua particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati:

procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono

modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi

modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave

prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro

procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi, nonché procedure per il salvataggio dei dati

modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali

Modalità operative da seguire per il trattamento dei dati

Al fine della corretta gestione dei dati in trattamento la invitiamo pertanto ad attenersi alle seguenti indicazioni:

richiedere e utilizzare soltanto i dati necessari alla normale attività lavorativa custodire i dati oggetto del trattamento in luoghi non accessibili a non autorizzati non lasciare incustodito il proprio posto lavoro prima di aver provveduto alla messa in sicurezza dei dati

non lasciare incustoditi e accessibili a terzi gli strumenti elettronici, mentre è in corso una sessione di lavoro procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni di consultazione

custodire e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici

accertarsi che i terzi siano a conoscenza e abbiano autorizzato l'uso dei dati richiesti accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita

non fornire telefonicamente o a mezzo fax dati senza specifica autorizzazione e/o identificazione del richiedente

Le presenti indicazioni sono tassative, la preghiamo di sottoscrivere la presente per presa visione in accettazione di quanto riportato.

Il titolare

Letto firmato e sottoscritto L'incaricato

Documento da predisporre per beneficiare del più lungo termine del 31 dicembre 2004 per adottare le nuove misure di sicurezza, introdotte dal d.lgs.19612003 e dal disciplinare tecnico di cui all'allegato b)

Il sottoscritto..... esercente l'attività di..... con sede in
..... codice fiscale.....

Premesso che:

effettua trattamenti di dati personali utilizzando strumenti elettronici;
alcuni di questi strumenti richiedono interventi per essere adeguati all'adozione delle nuove misure di sicurezza introdotte dal D.Lgs.19612003 e dal disciplinare tecnico di cui all'Allegato B).

Al fine di beneficiare del maggior termine disposto dai commi 2 e 3 dell'articolo 180 del D.Lgs. 19612003 per il completamento del processo di adozione delle nuove misure di sicurezza dichiara quanto segue:

(descrivere..gli..strumenti..elettronici..inadeguati,..e, , per.. ognuno,..le..ragioni..obiettive..di..tale inadeguatezza, gli interventi previsti, in che cosa consistono, quali tempi richiedono e la spesa preventivata)

Luogo e data

Firma del titolare

N.B. Il documento deve avere data certa, fornita anche con l'autoprestazione postale, oltre che con la registrazione, l'autentica della firma, ecc.