

SIENA AMBIENTE S.p.A.

*Sede legale: Poggibonsi (SI), Via Salceto 55
Sede Amministrativa: Siena, Str. Massetana Romana 58/D
Capitale Sociale: Euro 2.866.575,00 i.v.
C.F./R.I. di Siena n. 00727560526*

Documento Programmatico sulla Sicurezza delle Informazioni

- Art. 34 e Allegato B, regola 19, del D. Lgs. 30 giugno 2003, n. 196 -

- anno 2005 -

SOMMARIO

1	INTRODUZIONE	4
2	PRINCIPI GENERALI	5
3	TRATTAMENTO DATI PERSONALI.....	7
4	ORGANIZZAZIONE DEL TRATTAMENTO	11
4.1	LE FIGURE DI RIFERIMENTO	12
4.1.1	<i>Il Titolare del trattamento</i>	12
4.1.2	<i>I Responsabili del trattamento.....</i>	12
4.1.3	<i>Gli Incaricati del Trattamento.....</i>	13
4.2	DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ.....	14
5	ANALISI DEI RISCHI CHE INCOMBONO SUI DATI.....	18
6	MISURE MINIME ADOTTATE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI	26
6.1	PROTEZIONE DELLE AREE E DEI LOCALI	29
6.2	CRITERI E PROCEDURE PER L'ASSICURAZIONE DELLA INTEGRITÀ DEI DATI.....	30
7	TRATTAMENTO DEI DATI CON L'AUSILIO DI SUPPORTO CARTACEO	33
8	DESCRIZIONE DEL SISTEMA INFORMatico	35
8.1	SERVER E SISTEMI MULTI UTENTI:.....	35
8.2	RETI LOCALI ED ALTRI SISTEMI DI COLLEGAMENTO TERMINALI	35
8.3	PERSONAL COMPUTER.....	35
8.4	PERSONAL COMPUTER PORTATILI.....	36
8.5	UNITÀ DI ACCESSO PER GLI OPERATORI	36
8.6	DISPOSITIVI DI CONNESSIONE VERSO L'ESTERNO	36
8.7	COLLEGAMENTI DEL SISTEMA A DISPOSITIVI DI ACQUISIZIONE DATI.....	36
	ALLEGATO	39
	DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (ARTT. DA 33 A 36 DEL CODICE).....	39
	DEFINIZIONI (ART. 4 D. LGS 196/2003).....	43

Revisioni

Indice delle revisioni

Rev.	Data	Descrizione	Redatto	Verificato	Approvato

1 Introduzione

Il presente documento, redatto ai sensi del D. Lgs. 196/2003 e del disciplinare tecnico allegato al medesimo decreto [da qui in avanti anche 'Legge' o 'Codice'], è stato elaborato al fine di:

1. individuare i dati personali che sono trattati da Siena Ambiente S.p.A. ed il tipo di trattamento;
2. definire l'organizzazione per il trattamento e la protezione dei dati personali, sensibili e non, individuando il Titolare, il Responsabile e gli Incaricati per ogni tipo di trattamento;
3. rendere espliciti i criteri tecnici ed organizzativi applicati per la protezione delle aree e dei locali interessati alla tutela di dati personali;
4. organizzare, predisporre e soddisfare tutte le misure di sicurezza che debbono essere adottate, anche in via preventiva, da tutti gli operatori che trattano tali dati;
5. fornire una adeguata valutazione sul sistema di protezione degli stessi e sui criteri adottati per la salvaguardia della loro integrità.

Le regole contenute nel presente documento sono applicate all'interno della società Siena Ambiente S.p.A., titolare, ai sensi della Legge, del trattamento dei dati personali gestiti.

I Riferimenti normativi sono:

CODICE IN MATERIA DI DATI PERSONALI (D. Lgs. 30-6-2003 n. 196).

DISCIPLINARE tecnico in materia di misure minime di sicurezza (Artt. da 33 a 36 del Codice).

2 Principi Generali

Siena Ambiente S.p.A., nell'ambito della propria attività e della propria organizzazione, effettua il trattamento dei dati personali secondo le regole e le strutture organizzative di seguito specificate. Il presente documento individua i dati personali ed il tipo di trattamento, l'organizzazione aziendale preposta e, raccoglie e fornisce le regole e le informazioni utili per l'identificazione delle misure di sicurezza, organizzative, fisiche e logistiche, previste per la tutela dei dati trattati.

Siena Ambiente S.p.A., è strutturata in modo da:

1. Garantire il rispetto e le regole di cui al Titolo III del codice e garantire i diritti di cui al Titolo II dello stesso
2. Minimizzare la probabilità di appropriazione, danneggiamento o distruzione -anche involontaria- di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali;
3. Minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali;
4. Minimizzare la probabilità che i trattamenti dei dati personali siano modificati e/o usati senza autorizzazione.

Le misure di sicurezza organizzative, fisiche e logistiche, poste a tutela del trattamento dei dati, prevedono l'implementazione dei seguenti elementi:

1. strutture funzionali al trattamento dei dati;
2. singole responsabilità;
3. analisi e elenco dei trattamenti dei dati personali;
4. sistema informatico aziendale;
5. criteri tecnici ed organizzativi approntati al fine di proteggere le aree e i locali che custodiscono tali dati;
6. procedure predisposte per il controllo all'accesso ai dati delle persone autorizzate e per le modalità di custodia degli stessi durante il loro utilizzo;
7. descrizione dei criteri adottati per garantire le misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

Il sistema organizzativo è costruito in modo da rimuovere, nel minor tempo possibile, ogni eventuale situazione di deviazione accertata rispetto a quanto disciplinato nel presente documento. A tal fine il titolare si obbliga ad adottare le misure minime di sicurezza ed assumere il livello minimo di protezione dei dati personali a norma dell'art. 33 del Codice.

Il presente documento, ai fini del trattamento e della sicurezza dei dati, disciplina tutta la struttura di Siena Ambiente S.p.A.. E' applicato in tutta la sua organizzazione ed è oggetto di formazione ed aggiornamento professionale interno.

Ha validità annuale ed, entro il 31 marzo di ogni anno, sarà oggetto di revisione al fine di adeguarlo alle eventuali variazioni del livello di rischio a cui sono soggetti i dati personali e alle eventuali modifiche della tecnologia informatica e della normativa in materia.

Si applica al trattamento di tutti i dati personali:

- comuni;
- sensibili;
- giudiziari.

effettuati per mezzo di:

- strumenti elettronici di elaborazione.
- altri strumenti di elaborazione.

3 Trattamento dati personali

La società Siena Ambiente S.p.A, con sede legale in Via Salceto, 55 -53036 Poggibonsi (SI) e sede amministrativa in Siena, Str. Massetana Romana 58/D 53100 - Cod. Fis. e Partita I.V.A 00727560525, iscritta al registro delle Imprese di Siena al n. 6609/8416, per lo svolgimento delle proprie funzioni economiche, tecniche e gestionali descritte nell'oggetto sociale, tratta una molteplicità di dati tra cui dati sensibili e, in alcuni casi particolari, dati definiti dalla legge 'giudiziari', per i quali la normativa impone specifiche misura di sicurezza.

In particolare, il trattamento dei dati in possesso di Siena Ambiente SpA è sintetizzabile nel seguente elenco:

1. Trattamento di dati genetici:
 - Dati idonei ad accertare maternità o paternità;
 - Dati relativi ad indagini epidemiologiche ed a rilevare lo stato di salute.
2. Trattamento di dati sensibili limitati a quelli necessari per assolvere obblighi normativi e contrattuali :
 - Dati relativi alla Iscrizione a organismi sindacali.
3. Trattamento di dati che indicano la posizione geografica di persone o beni strumentali aziendali mediante una rete di comunicazione elettronica:
 - Dati idonei a rilevare la posizione di persone;
 - Dati idonei a rilevare la posizione di beni, strumenti, oggetti.
4. Trattamento di dati giudiziari necessari per assolvere agli obblighi normativi e di legge (es. normativa appalti pubblici) acquisiti anche in apposite banche dati di enti di controllo o autorità indipendenti gestite con strumenti elettronici
5. Trattamento dati relativi ad altri provvedimenti o procedimenti giudiziari;
6. Trattamento dati personali elaborati sistematicamente con supporti cartacei ed informatici;

In generale vengono trattati dati personali comunque riferiti a persone fisiche o persone giuridiche che hanno rapporti finanziari, commerciali, di lavoro o di collaborazione con Siena Ambiente S.p.A.

In particolare il trattamento dei dati sopra indicati, interessano le seguenti categorie di persone:

- personale dipendente, compresa l'iscrizione ad organizzazioni sindacali, limitatamente all'adempimento degli obblighi di legge e contrattuali;
- professionisti e lavoratori autonomi;
- candidati a selezioni per l'instaurazione di un rapporto di lavoro;
- amministratori e soci, anche di società collegate e partecipate;
- clienti ed utenti, anche potenziali;
- fornitori di beni e servizi, anche potenziali;
- enti o organismi pubblici;

I dati sono gestiti per la maggior parte tramite elaboratori informatici, collegati in rete intranet, e predisposti per collegamento a internet e posta elettronica.

All'interno del sistema intranet, i dati sono raggruppati in un archivio informatico suddiviso in cartelle/directory e più livelli di sottocartelle contenenti specifici file ed in strutture di database.

La struttura informatica, compreso i sistemi di protezione già in atto, può essere così sintetizzata:

Tab. 1. Archivio Dati

ARCHIVIO / DATA BASE	SISTEMA DI PROTEZIONE	CARTELLA	CATEGORIA DI DATO	SOTTOCARTELLA
ARC SI	È quello tipico del S.O. Windows 2000: l'accesso alle cartelle/sottocartelle è abilitato solo a soggetti dotati di credenziali di autenticazione	ASO	Dati personali/ dati genetici/ dati sensibili/ dati giudiziari	ASO-110 Tutela giudiziaria ASO-400 Sicurezza ASO-900 Personale
		ATO-8	/	
		Awe	/	
		Awe-SA	Dati personali/ dati genetici/ dati sensibili/ dati giudiziari	ASP
		Bioecologia	Dati personali/ dati genetici/ dati sensibili/ dati giudiziari	ASO PCO PER
		Cogesa	Dati personali/ dati genetici/ dati sensibili/ dati giudiziari	ASO -Organizzazione-Personale
		DATABASE	Dati personali/ dati genetici/ dati sensibili/	File CNA
		GES	/	
		ITEKO	Dati personali/ /	ASO-00P
		IT.OS	Dati personali	ASO 000P
		SRS	Dati personali /	SRI -SPZ
		STE	/	
		STR	Dati che indicano la posizione geografica di persone	STR 01
		Sys	/	
TIA	Dati personali	00- Diverse 01-Abbadia S. Salvatore 02-Asciano 06-Castelnuovo Berardenga 014-Montalcino 017-Monteroni D'Arbia 032-Siena 033-Sinalunga		
ARC PG	È quello tipico del S.O. Windows 2000: l'accesso alle cartelle/sottocartelle è abilitato solo a soggetti dotati di credenziali di autenticazione	CMP	/	
		DSC	Dati personali/ Dati giudiziari	Progetti - Appalto
		In giro	/	
		IRE	/	
		SEL	/	
		SPP	/	
		STS000	/	
		TRM	Dati personali/dati giudiziari	Progetti - Appalto
VAL	/			
SUPERGULP/DB	Si accede alle cartelle contenenti dati personali solo se abilitati		Dati personali/ dati sensibili/ dati che indicano la posizione geografica di persone	

Trattamento affidato all'esterno

Per la propria attività, Siena Ambiente S.p.A. si avvale anche della consulenza e collaborazione di società esterne cui è stato delegato il trattamento di alcuni dati personali.

L'attività delegata è la seguente:

- a) Amministrazione del personale: relativamente alla formulazione della busta paga e parte degli adempimenti amministrativi connessi con la gestione amministrativa del personale;
- b) Assistenza tecnica e sistemistica; gestione rete informatica; consulenza servizi informatici: manutenzione e eventuale aggiornamenti antivirus, sempre sotto la guida dell'ufficio informatico interno a Siena Ambiente S.p.A.
- c) Professionisti in materia giuridica, contabile e fiscale, edilizia e impiantistica;

I soggetti delegati sono i seguenti:

- per quanto attiene il precedente punto a)
 - **Cesam CNA** –Via delle Regioni 78 -53100 Siena, p.iva 00123720526;
- per quanto attiene il precedente punto b)
 - **Tosco Dati Siena S.r.l.** –Via Cassia Nord 106 -53035 Monteriggioni -Siena. –p.iva e c.f. 00790640528;
 - **Inforel S.r.l.** –Corso Mazzini 14 -27100 Pavia –p.iva 0155134083
- per quanto attiene il precedente punto c):
 - **Studio Legale Giallongo** –, Via Alfieri 19, 50121 Firenze –**Studio Legale Comporti** Via Pantaneto 7, 53100 Siena – **Studio Legale Tartaglione**, C.so Italia 20, 50123 Firenze – **Studio Commerciale Fabbrini Paolo**, Via Amman, 53021 Abbadia San Salvatore (SI)

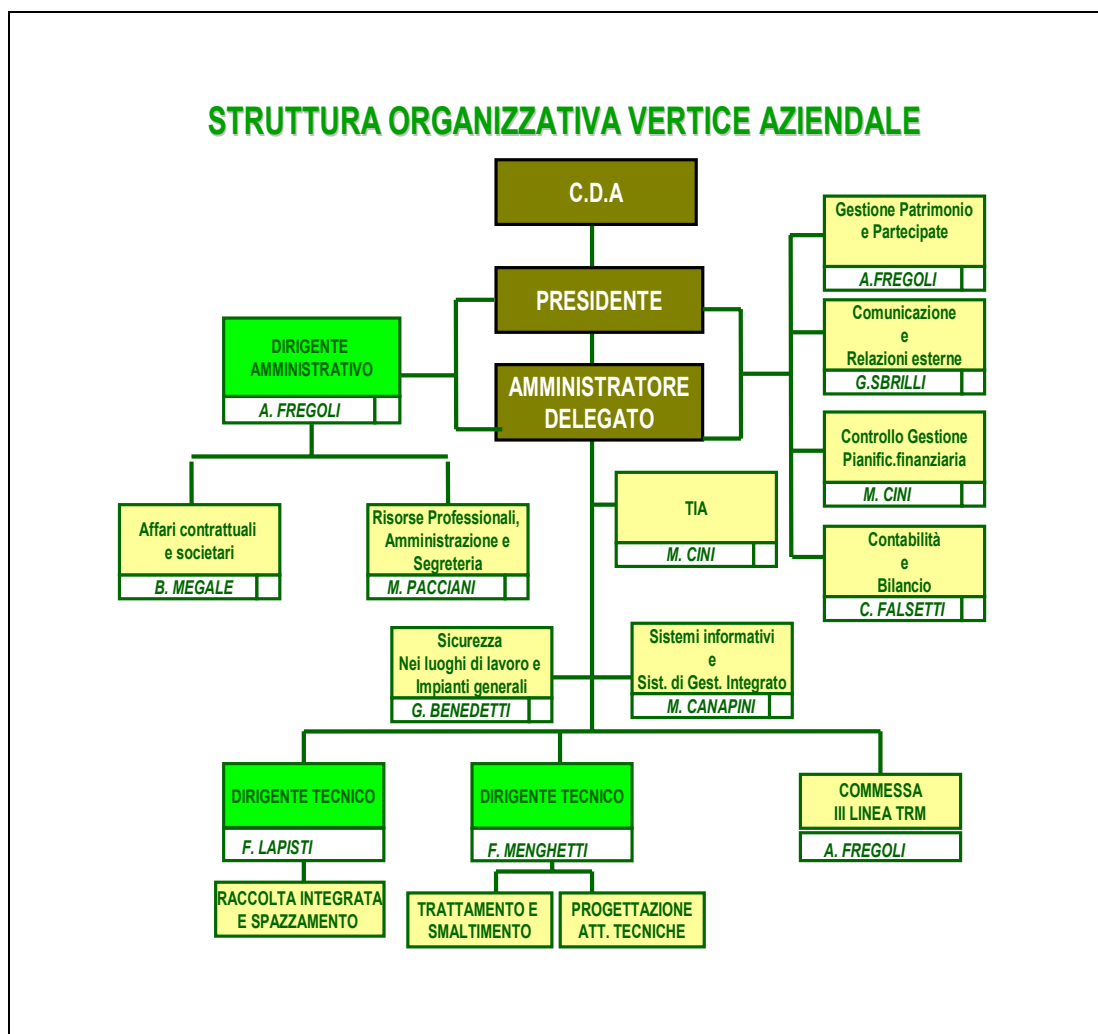
Categorie di dati interessati al trattamento svolto all'esterno:

- a) dati relativi al personale dipendente;
- b) eventuale accesso a tutti i dati comuni, personali, giudiziari e sensibili presenti nella rete informatica aziendale;

L'oggetto del trattamento esternalizzato riguarda i dati personali e i dati sensibili, relativi all'iscrizione a sindacati, mentre non riguarda il trattamento di dati giudiziari se non per la specifica attività legale.

4 Organizzazione del trattamento

Nell'ambito della organizzazione aziendale, illustrata dall'organigramma che segue, il trattamento e la sicurezza dei dati personali è svolta dal Titolare, dal Responsabile e dagli Incaricati.



4.1 Le figure di riferimento

4.1.1 Il Titolare del trattamento

A norma dell'art. 28 del Codice in materia di dati personali, il Titolare del Trattamento è Siena Ambiente S.p.A. nel suo complesso, nella persona del Legale Rappresentante.

Il Titolare del trattamento ha il compito di indirizzo e controllo sul rispetto delle norme del codice e del presente documento e sugli obblighi indicati nelle lettere di incarico ai Responsabili e agli Incaricati del trattamento dei dati personali, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di sicurezza dei dati personali.

Tenendo conto delle mansioni, della professionalità e delle attività svolte, della capacità e affidabilità, il Legale Rappresentante nomina Coordinatore dei Responsabili dei Trattamenti dei dati il Dirigente Dott. Albo Fregoli.

Il Titolare del Trattamento, informa ciascun Responsabile/Incaricato della sicurezza dei dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (D. Lgs. 30-6-2003 n. 196) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

4.1.2 I Responsabili del trattamento

Il Responsabile del Trattamento dei Dati Personali, ai fini della sicurezza, ha le seguenti funzioni:

- Promuove lo sviluppo, la realizzazione e l'aggiornamento dei programmi di sicurezza contenuti nel presente Documento Programmatico sulla Sicurezza dei Dati Personali;
- Informa il Titolare del Trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti proponendo le necessarie contromisure organizzative e procedurali;
- Promuove la formazione degli Incaricati del Trattamento e mantiene attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;
- Garantisce che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- Se il trattamento è effettuato con mezzi informatici, individua, nomina e incarica per iscritto, uno o più incaricati per la gestione e manutenzione degli strumenti elettronici e per la custodia delle copie delle credenziali di autenticazione;

- Se il trattamento è effettuato con mezzi non informatici (ad. es. in forma cartacea) il responsabile individua uno o più incaricati per la custodia e la salvaguardia dei dati personali.

Il responsabile del Trattamento ai sensi dell'art. 29 del Codice dirige gli incaricati al trattamento e garantisce il rispetto delle regole e dei diritti di cui al II e III Titolo del Codice e garantisce l'adozione delle misure di sicurezza ai sensi della normativa in materia tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previa idonee istruzioni fornite anche per iscritto.

La nomina del Responsabile del Trattamento della sicurezza dei Dati Personali è effettuata dal Titolare del Trattamento tramite disposizione organizzative contenente la specificazione delle modalità di effettuazione del trattamento dei dati e delle misure di sicurezza da osservare in relazione a quanto disposto dalle normative in vigore.

Copia della lettera di nomina, firmata per accettazione, è conservata, a cura del Titolare del Trattamento, in luogo conforme al presente DPS.

4.1.3 Gli Incaricati del Trattamento

Gli incaricati del trattamento dei dati personali sono preposti in modo esclusivo, ai sensi dell'art. 30 del Codice, al trattamento nei limiti della disposizione organizzativa di designazione e dal presente documento.

Gli Incaricati del Trattamento dei Dati Personali, con specifico riferimento alla sicurezza, si attengono alle seguenti regole:

- a) Non debbono lasciare in nessun caso incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dati personali;
- b) Debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti o i documenti contenenti dati personali;
- c) Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate;

- d) Deve adottare tutte le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia dei dispositivi in possesso ed a uso esclusivo dell'incaricato;
- e) Hanno l'obbligo di assoluta riservatezza.

Gli incaricati del trattamento dei dati personali rispettano e fanno rispettare le regole generali per il trattamento dei dati personali di cui al Titolo III del D. Lgs. 196/2003.

Essi non modificheranno i trattamenti esistenti o introdurranno nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del trattamento.

La nomina di ciascun Incaricato del Trattamento della sicurezza dei Dati Personali è effettuata dal Responsabile del Trattamento, con una disposizione organizzativa, contenente la specificazione delle responsabilità affidate. La lettera di nomina, controfirmata per accettazione dall'interessato, è conservata in luogo conforme al presente DPS.

4.2 Distribuzione dei compiti e delle responsabilità

All'interno di Siena Ambiente S.p.A. sono preposti al trattamento dei dati personali i seguenti uffici e relativo personale:

Tab. 2. Distribuzione Compiti

SERVIZIO	RESPONSABILE	INCARICATO
Servizio Risorse Professionali, Amministrazione e Segreteria	Pacciani Marina	Alessandra Mancini - Marco Parigi - Corti Simona – Brogi Maria Elena
Servizio Contabilità e Bilancio	Falsetti Claudia	Stefania Badaloni - Capezuoli Barbara –Francesca Pierini
Servizio Trattamento, Smaltimento e Progettazione	Menghetti Fabio	Biagini Alessio- Bimonte Pasquale Elisabetta Centini –Mangiavacchi Silvia
Servizio Raccolta Integrata e Spazzamento	Fabio Lapisti	Alborè Nicoletta -Angelini Monia – Muzzetto Nicolò – Ranieri Gianluca – Rossi Nicola
Servizio Controllo di gestione e Pianificazione Finanziaria	Cini Massimo	Lipira Graziella

Documento Programmatico sulla Sicurezza - 2005

Servizio Tariffa Igiene Ambientale	Cini Massimo	Antidormi Michela
Servizio Affari Contrattuali e Societari	Megale Bruno Antonio	Giordano Chechi –Becatti Carlo – Di Giacomantonio Alessio
Servizio Sicurezza nei Luoghi di Lavoro e Impianti Generali	Benedetti Giovanni	Gistri Valentina –Giuliana Pirrone
Servizio Sistemi informativi e Sistema di Gestione Integrato	Canapini Masco	Travaglini Claudio
Servizio Comunicazione e Relazioni Esterne	Sbrilli Giorgio	Roccioletti Erika

Per il trattamento dei dati personali, il Titolare nominerà per iscritto i Responsabili del Trattamento mentre gli incaricati del trattamento saranno nominati per iscritto dal responsabile e, in forma congiunta, dal Titolare stesso.

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

I compiti, le funzioni e le relative responsabilità delle strutture preposte al trattamento dei dati (comuni, sensibili, giudiziari) effettuati, sono descritti nella seguente sezione:

Tab. 3. Competenze e responsabilità delle strutture preposte al trattamento

STRUTTURA	RESPONSABILE	TRATTAMENTO EFFETTUATO	DEFINIZIONE DEI COMPITI E DELLE FINALITÀ DELLA STRUTTURA
Servizio Risorse Professionali, Amministrazione e Segreteria	Marina Pacciani	Raccolta dati anagrafici; dati comuni relativi a clienti/utenti; dati comuni relativi a fornitori; dati relativi ad altri soggetti Gestione contratti; dati di natura giudiziaria; dati anagrafici	Acquisizione e caricamento dei dati; comunicazione alle altre strutture interne Consultazione - Comunicazione anche esterna a seguito di specifica richiesta o autorità competenti
Servizio Contabilità e Bilancio	Claudia Falsetti	Dati fiscali e contabili; dati relativi allo svolgimento di att. Econom./comm. con fornitori e clienti;	Programmi di gestione della contabilità; archivi utilizzati esclusivamente per rapporti di carattere commerciale
Servizio Trattamento, Smaltimento e Progettazione	Menghetti Fabio	Dati anagrafici per lo svolgimento attività di gestione	Acquisizione e caricamento dei dati; comunicazione alle altre strutture interne
Servizio Raccolta Integrata e Spazzamento	Fabio Lapisti	Dati idonei a rilevare la posizione di persone,	Gestione personale/ forme di sicurezza

Documento Programmatico sulla Sicurezza - 2005

		strumenti ed oggetti;	privata/ difesa del suolo, igiene urbana o tutela dell'ambiente
Servizio Tariffa Igiene Ambientale Controllo di gestione e pianificazione finanziaria	Cini Massimo	Dati anagrafici per lo svolgimento attività economica	Acquisizione e caricamento dei dati; comunicazione alle altre strutture interne
Servizio Affari Contrattuali e Societari	Megale Bruno Antonio	Dati anagrafici per lo svolgimento attività di gestione	Acquisizione e caricamento dei dati; comunicazione alle altre strutture interne
Servizio Sicurezza nei Luoghi di Lavoro e Impianti Generali	Benedetti Giovanni	Dati anagrafici, dati relativi allo stato di salute dei dipendenti	Gestione tecnica operativa delle norme di sicurezza;
Servizio Sistemi Informativi e Sistema di Gestione Integrato	Canapini Masco	Controllo dati elaborati in rete;	Manutenzione tecnica della struttura informatica, elaborazione informatica dei dati e sicurezza struttura;
Servizio Comunicazione e Relazioni Esterne	Sbrilli Giorgio	Dati anagrafici per lo svolgimento attività di gestione	Acquisizione e caricamento dei dati; comunicazione alle altre strutture interne

Tab. 4. Elenco dei Trattamenti: Informazioni essenziali

FINALITÀ PERSEGUITA O ATTIVITÀ SVOLTA	CATEGORIA DI INTERESSATO	NATURA DATI TRATTATI: DATO PERSONALE -DP- / SENSIBILE -DS- / GIUDIZIARIO -DG-			STRUTTURA DI RIFERIMENTO	DESCRIZIONE DEGLI STRUMENTI UTILIZZATI
Raccolta dati	Personale dipendente; clienti; lavoratori autonomi; associati iscritti; potenziali clienti; fornitori artigiani; imprenditori; piccoli imprenditori; soggetti o organismi pubblici;	DP	/	/	Servizio protocollo e segreteria	Elaboratori o p.c portatili in rete privata; Cartaceo
Gestione dati per attività amministrativa	Personale dipendente; lavoratori autonomi; associati iscritti; fornitori; imprenditori; piccoli imprenditori; soggetti o organismi pubblici; candidati da considerare per l'instaurazione di un rapporto di lavoro; o soggetti che avranno rapporti commerciali con la società.	DP	DS	DG	Incaricato di rilevazioni e prestazioni di servizi	Elaboratori o p.c portatili in rete privata; Cartaceo
Gestione dati per servizio contabilità	Personale dipendente; clienti; lavoratori autonomi; associati iscritti; fornitori artigiani; imprenditori; piccoli imprenditori; soggetti o organismi pubblici;	DP	DS	/	Addetti alla contabilità ed alla fatturazione	Elaboratori o p.c portatili in rete privata; Cartaceo
Gestione sistema dati raccolti per attività informatica e attività di controllo	Personale dipendente; clienti; lavoratori autonomi; associati iscritti; fornitori artigiani; imprenditori; piccoli imprenditori; soggetti o organismi pubblici;	DP	DS	/	Addetti alla struttura informatica	Elaboratori o p.c portatili in rete privata
Dati idonei a rilevare la posizione di persone, beni, strumenti. Per ottimizzare gli aspetti gestionali/operativi	Dipendenti/collaboratori Passeggeri su veicoli o utenti di mezzi trasporto.	DP	/	/	Servizio raccolta	Raccolta tramite sistema satellitare; Elaboratori o p.c portatili in rete privata

5 Analisi dei rischi che incombono sui dati

L'analisi dei possibili rischi che gravano sui dati è stata effettuata combinando due tipi di rilevazioni:

- 1) La tipologia dei dati trattati, nonché la pericolosità per la privacy dei soggetti cui essi si riferiscono;
- 2) Le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

Siena Ambiente S.p.A. ha individuato come fonte di rischio che può incombere sui dati le seguenti categorie di eventi potenzialmente dannosi:

- **Comportamento degli operatori :**
 - Sottrazione di credenziali di autenticazione;
 - Carenza di consapevolezza, disattenzione o incuria;
 - Comportamenti sleali o fraudolenti;
 - Errore materiale e nella gestione della sicurezza fisica;

- **Eventi relativi agli strumenti :**
 - Azione di virus informatici o di programmi suscettibili di recare danno;
 - Spamming o tecniche di sabotaggi;
 - Malfunzionamento, indisponibilità o degrado degli strumenti;
 - Accessi esterni non autorizzati;
 - Intercettazione di informazioni in rete;

- **Eventi relativi al contesto:**
 - Accessi non autorizzati a locali/reparti ad accesso ristretto;
 - Sottrazione di strumenti contenenti dati;
 - Guasto sistema complementare;
 - Eventi distruttivi, naturale o artificiale (allagamenti, incendi, etc)

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

- 1) La situazione delle apparecchiature hardware installate con cui vengono trattati i Dati;
- 2) La situazione delle apparecchiature periferiche;
- 3) La situazione dei dispositivi di collegamento con reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- 1) La sicurezza dei dati trattati;
- 2) Il rischio di distruzione o di perdita;
- 3) Il rischio di accesso non autorizzato.

oltre che monitorare la situazione dei sistemi operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

I responsabili della gestione e della manutenzione degli strumenti elettronici nel caso in cui esistano rischi evidenti informano il Responsabile della Sicurezza dei Dati Personali, perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

La valutazione della gravità di ciascun evento e le possibili conseguenze per la sicurezza dei dati in relazione a ciascun fattore di rischio, sono così sintetizzate:

Tab. 5. Analisi dei rischi.

N. EVENTO	DESCRIZIONE EVENTO	SI/NO	PROB.*	DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA (gravità: alta/media/bassa)*	VALORE (IR)*	VALUTAZ. DEL RISCHIO
COMPORAMENTO DEGLI OPERATORI						
1 Sottrazione di credenziali di autenticazione	Le credenziali (userID/Password) possono essere sottratte al legittimo possessore con vari metodi, anche grazie alla negligenza nella conservazione da parte del possessore stesso	SI	2	Media Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto o in parte al soggetto possessore delle stesse. Il sistema di protezione non può sapere in principio dell'occorrenza di tale furto	4	Tollerabile
2 Carenza di consapevolezza, disattenzione o incuria	Le credenziali (userID/Password) possono essere sottratte al legittimo possessore con vari metodi, anche grazie alla negligenza nella conservazione da parte del possessore stesso	SI	1	Media Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto o in parte al soggetto possessore delle stesse. Il sistema di protezione non può sapere in principio dell'occorrenza di tale furto	2	Accettabile
3 Comportamenti sleali o fraudolenti	Con comportamento consapevole, derivante potenzialmente da vari fattori (es. risentimenti verso la Società, il perseguimento di fini personali, etc.) gli incaricati del trattamento possono compiere operazioni illecite sulla banca interessata all'evento	SI	2	Alta Nei casi più gravi si può ottenere la distruzione di tutta o parte la banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione , in modo illecito, dei dati.	6	Inaccettabile

N. EVENTO	DESCRIZIONE EVENTO	SI/NO	PROB.*	DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA <hr/> (gravità: alta/media/bassa)*	VALORE (IR)*	VALUTAZ. DEL RISCHIO
4 Errore materiale e nella gestione della sicurezza fisica;	A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli addetti al trattamento possono compiere operazioni errate o specificare dati errati	SI	2	Media Nei casi più gravi si può ottenere la distruzione di tutta o parte la banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati.	4	Tollerabile
EVENTI RELATIVI AGLI STRUMENTI						
5 Azione di virus informatici o di programmi suscettibili di recare danno	Sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può venirsi ad installare o essere semplicemente eseguito dal software spurio del tipo "virus" informatico	SI	3	Media Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, dei dati.	6	Inaccettabile
6 Spamming o tecniche di sabotaggi	Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta spuria generata anche con strumenti automatizzati. Tali messaggi possono contenere false notizie.	SI	3	Bassa Gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non regolari	3	Accettabile
7 Malfunzionament o, indisponibilità o degrado degli strumenti	I sistemi con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da cui possono derivare azioni reali sui dati parzialmente o	SI	1	Bassa Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati.	1	Trascurabile

N. EVENTO	DESCRIZIONE EVENTO	SI/NO	PROB.*	DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA <hr/> (gravità: alta/media/bassa)*	VALORE (IR)*	VALUTAZ. DEL RISCHIO
	totalmente diverse da quelle che si volevano operare					
8 Accessi esterni non autorizzati	Soggetti in possesso di credenziali di accesso al sistema, o intenzionati a sferrare un attacco informatico ad uno dei sistemi da cui è possibile intervenire su una banca dati obiettivo, possono accedere al sistema individuato da una postazione non utilizzata in condizioni normali di operatività per accedere a tale sistema	SI	2	Alta Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.	6	Inaccettabile
9 Intercettazione di informazioni di rete	Soggetti esterni possono catturare, mediante vari sistemi fisici, parte delle informazioni che transitano sulla rete informatica della società	SI	1	Media Nei casi più gravi mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione dei dati da parte di malintenzionati	2	Accettabile
EVENTI RELATIVI AL CONTESTO						
10 Accessi non autorizzati a locali/reparti ad accesso ristretto	Un soggetto autorizzato allo scopo, può comunque accedere fisicamente al locali presso dei quali è accessibile e manipolabile la banca dati interessata all'evento	SI	1	Alta Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione , in modo illecito, dei dati.	3	Accettabile

N. EVENTO	DESCRIZIONE EVENTO	SI/NO	PROB.*	DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA <hr/> (gravità: alta/media/bassa)*	VALORE (IR)*	VALUTAZ. DEL RISCHIO
11 Sottrazione di strumenti contenenti dati	I sistemi e/o supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono venire sottratti illecitamente da parte di altri soggetti non aventi diritto di accedere a tale banca dati	SI	1	Media L'evento comporta la sottrazione, in modo illecito, di dati.	2	Accettabile
12 Guasto sistema complementare	I sistemi ausiliari necessari al corretto funzionamento degli apparati con i quali viene trattata o che contiene la banca dati interessata all'evento possono avere malfunzionamenti in conseguenza di varie cause	SI	1	Media Dall'evento può derivare la distruzione totale o parziale della banca dati	2	Accettabile
13 Eventi distruttivi, naturale o artificiale (allagamenti)	I sistemi o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono essere interessati da eventi distruttivi di origine sia fortuita che dolosa	SI	1	Media Dall'evento può derivare la distruzione totale o parziale della banca dati	2	Accettabile

***Identificazione e valutazione rischi:**

1. Gravità del danno

Impatto rischio	Descrizione	Indice numerico
Bassa	Manipolazione parziale dati	1
Media	Sottrazione illecita dei dati	2
Alta	Distruzione di tutta o parte banca dati: -sottrazione illecita dei dati -distruzione totale o parziale banca dati	3

2. Probabilità

Probabilità	Indice numerico	Descrizione
Poco probabile	1	-Il fattore di rischio può verificarsi solo in circostanze occasionali o sfortunate di eventi; -Non sono noti o sono rari episodi già verificatisi; -Non esiste nessuna correlazione tra attività lavorativa e fattori di rischio;
Probabile	2	-Il fattore di rischio può recare un danno anche se non in maniera automatica o diretta; -Esiste una correlazione tra attività e/o fattore di rischio;
Altamente probabile	3	-Si registrano danni per tipologia considerata; -L'attività lavorativa richiede una particolare organizzazione del lavoro perché presenta interferenze, sovrapposizioni, incompatibilità di operazioni; -Sono state segnalate situazioni di rischio potenziale per danni gravi

3. Entità del rischio (Prob. X Gravità)

Scala	Gravità		
	bassa	media	alta
Probabilità			
Poco probabile	1	2	3
Probabile	2	4	6
Altamente probabile	3	6	9

4. Valore IR [Indice del rischio ponderato tra la probabilità dell'evento e la sua gravità]

Evento	Probabilità	Gravità	Valore (IR)
1	Probabile	Media	4
2	Poco probabile	Media	2
3	Probabile	Alta	6
4	Probabile	Media	4
5	Altament.Probabile	Media	6
6	Altament.Probabile	Bassa	3
7	Poco probabile	Bassa	1
8	Probabile	Alta	6
9	Poco probabile	Media	2
10	Poco probabile	Alta	3
11	Poco probabile	Media	2
12	Poco probabile	Media	2
13	Poco probabile	Media	2

5. Misure di Contrasto (indica le attività da effettuare sulla base della valutazione del rischio)

Entità del rischio corretta	Valutazione del rischio	Definizione
1	Trascurabile	Il rischio potenziale è sotto controllo
$1 < IR < 4$	Accettabile	Il rischio è talmente ridotto da non dovere essere preso in esame a meno che non sia facilmente eliminabile. Se non viene eliminato andrà comunque indicato come rischio residuo
$4 \leq IR < 6$	Tollerabile	Il rischio è tale da dovere essere preso in considerazione e, se possibile, eliminato o ridotto al massimo grado. Qualora non sia possibile eliminare o ridurre il rischio, il medesimo può essere accettato come rischio residuo
$IR \geq 6$	Inaccettabile	Se il rischio non può essere eliminato o ridotto la condizione lavorativa associata a tale rischio non può sussistere e deve essere eliminata

6 Misure minime adottate per garantire l'integrità e la disponibilità dei dati

Alla luce dei fattori di rischio e delle aree individuate nel precedente paragrafo, vengono descritte le misure atte a garantire:

- 1) La protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- 2) La corretta archiviazione e custodia dei dati;
- 3) La sicurezza logica, nell'ambito degli strumenti elettronici.

Le misure indicate a sostegno della fase di protezione dei dati sono già adottate al momento della stesura del presente documento e sono del seguente tipo:

Tab. 6. Misure di protezione

TIPOLOGIA	DESCRIZIONE TIPOLOGIA
Organizzativa	<ol style="list-style-type: none"> a) Prescrizione di linee guida di sicurezza; b) Assegnazione di incarichi; c) Classificazione dei dati.
Fisico	<ol style="list-style-type: none"> a) Vigilanza della sede; b) Ingresso controllato nei luoghi dove avviene l'elaborazione ed il trattamento dei dati; c) Controllo sull'operato degli addetti alla manutenzione; d) Verifica della leggibilità dei supporti.
Procedurale	<ol style="list-style-type: none"> a) Identificazione dell'incaricato e/o utente, attraverso un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici; b) Controlli aggiornati antivirus al fine di proteggere gli strumenti e dati da malfunzionamenti e attacchi informatici; c) Annotazione del responsabile dell'operazione, con autorizzazione e definizione delle tipologie di dati ai quali gli stessi incaricati possono accedere al fine delle proprie mansioni lavorative; d) Verifiche periodiche su dati o trattamenti non consentiti o non corretti; e) Controllo sull'operato degli addetti alla manutenzione; f) Controllo sui supporti consegnati in manutenzione al fine di prescrivere le opportune cautele per la custodia e l'utilizzo dei supporti rimovibili.

Tab. 7. Misure di sicurezza

A) Comportamento degli operatori

STRUTTURE INTERESSATE	DESCRIZIONE RISCHI CONTRASTATI	TRATTAMENTI INTERESSATI	DESCRIZIONE MISURA GIÀ IN ESSERE	STRUTTURE O PERSONE ADDETTE ALL'ADOZIONE
COMPORAMENTO DEGLI OPERATORI				
TUTTE LE STRUTTURE DELLA SOCIETA', OLTRE A RISCHI CONNESSI ALLE STRUTTURE HARDWARE, ALLE RISORSE SOFTWARE, RISCHI SULLE RISORSE DATI	Sottrazione credenziali di autenticazione	<u>Tutti i tipi di dati</u>	Le macchine sono in buono stato e sono utilizzate esclusivamente da personale autorizzato; l'accesso alle risorse dati è protetto dall'uso di password personali	Servizio sicurezza e struttura informatica
	Carenza di consapevolezza, disattenzione o incuria			
	Comportamenti sleali o fraudolenti			
	Errore materiale			
	Errore nella gestione della sicurezza fisica	<u>Tutti i tipi di dati</u>	Istruzioni scritte	

B) Eventi relativi agli strumenti

STRUTTURE INTERESSATE	DESCRIZIONE RISCHI CONTRASTATI	TRATTAMENTI INTERESSATI	DESCRIZIONE MISURA GIÀ IN ESSERE	STRUTTURE O PERSONE ADDETTE ALL'ADOZIONE
EVENTI RELATIVI AGLI STRUMENTI				
TUTTE LE STRUTTURE DELLA SOCIETA', OLTRE A RISCHI CONNESSI ALLE STRUTTURE HARDWARE, ALLE RISORSE SOFTWARE, RISCHI SULLE RISORSE DATI	Malfunzionamento, indisponibilità o degrado degli strumenti	<u>Tutti i tipi di dati</u>	Le macchine sono in buono stato e sono utilizzate esclusivamente da personale autorizzato e sottoposte a controlli periodici effettuati da tecnici competenti	Servizio sicurezza e struttura informatica
	Accessi esterni non autorizzati	<u>Tutti i tipi di dati</u>	Al termine dell'orario di lavoro tutti gli uffici sono chiusi e viene attivato il sistema di allarme per la rilevazione di eventuali intrusioni esterne; le macchine sono	Servizio sicurezza e struttura informatica

			protette da password personali modificate periodicamente	
	Intercettazione di informazioni in rete	<u>Tutti i tipi di dati</u>	Utilizzo programmi antivirus; il collegamento con il modem è limitato all'esterno solo al tempo necessario per le operazioni gestionali, sono effettuati salvataggi periodici dei dati archiviati; alle risorse dati non accedono persone non autorizzate e la manutenzione è effettuata da tecnici di fiducia	Servizio sicurezza e struttura informatica
	Azione di virus informatici o di programmi suscettibili di recare danno			
	Spamming o tecniche di sabotaggi			

C) Eventi relativi al contesto

STRUTTURE INTERESSATE	DESCRIZIONE RISCHI CONTRASTATI	TRATTAMENTI INTERESSATI	DESCRIZIONE MISURA GIÀ IN ESSERE	STRUTTURE O PERSONE ADDETTE ALL'ADOZIONE
EVENTI RELATIVI AL CONTESTO				
TUTTE LE STRUTTURE DELLA SOCIETÀ, OLTRE A RISCHI CONNESSI ALLE STRUTTURE HARDWARE, ALLE RISORSE SOFTWARE, RISCHI SULLE RISORSE DATI	Eventi distruttivi, naturali o artificiali (allagamenti, incendi, ecc)	<u>Tutti i tipi di dati</u>	Per il pericolo di allagamenti i server sono in posizione rialzata da terra; negli uffici esiste un sistema di rilevazione anti-incendio; si dispone di un gruppo di continuità per assicurare l'erogazione di energia elettrica; impianto elettrico a norma	Servizio sicurezza e struttura informatica
	Accessi non autorizzati a locali/reparti ad accesso ristretto	<u>Tutti i tipi di dati</u>	Al termine dell'orario di lavoro tutti gli uffici sono chiusi e viene attivato il sistema di allarme per la rilevazione di eventuali intrusioni esterne; le macchine sono protette da password personali modificate periodicamente	Servizio sicurezza e struttura informatica

	Sottrazione di strumenti contenenti dati; Guasto sistema complementare	<u>Tutti i tipi di dati</u>	Sono effettuati salvataggi periodici dei dati archiviati; alle risorse non accedono persone non autorizzate e la manutenzione è effettuata da tecnici di fiducia	Servizio sicurezza e struttura informatica
--	---	------------------------------------	--	--

6.1 Protezione delle aree e dei locali

Il furto o il danneggiamento delle apparecchiature informatiche, la diffusione o la distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre Siena Ambiente S.p.A al rischio di non rispettare quanto previsto nel D. Lgs. 196/2003.

Per ovviare a simili eventualità, sono state applicate le seguenti misure di sicurezza:

- i locali sono dotati di un impianto di allarme a sensori infrarossi che si disinserisce solo attraverso una chiave magnetica in possesso solo dei dipendenti. La lista dei possessori è conservata ed aggiornata a cura del servizio sicurezza. Il sistema di protezione viene attivato al termine dell'orario di lavoro;
- l'azienda è, inoltre, dotata di un sistema di comunicazione telefonica di allarme, che consente, nel caso di intrusione di soggetti non autorizzati in situazione di non presidio, un collegamento diretto con la stazione dei carabinieri mediante l'attivazione di una chiamata automatica;
- le aree contenenti il supporto cartaceo (archivio e mobili contenenti documentazione contabili dei clienti della società medesima) sono protette in modo da evitare il tentativo di accesso da parte di persone estranee;
- l'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Sistemi di registrazione degli accessi e delle uscite dei dipendenti

All'atto dell'entrata e dell'uscita nei locali aziendali il dipendente è tenuto a segnalare la propria presenza tramite l'utilizzo del badge magnetico personale in dotazione, mentre un sistema di videocitofono consente il controllo della presenza degli esterni.

Dispositivi antincendio

La sede aziendale è dotata di estintori a polvere e ad anidride carbonica per l'utilizzo con apparecchiature informatiche. Un estintore ad anidride carbonica è situato nei pressi della sala server aziendale.

6.2 Criteri e procedure per l'assicurazione della integrità dei dati

Il sistema informatico all'interno del quale sono conservati i dati personali è protetto dall'intrusione esterna alla rete aziendale tramite le tecnologie di sicurezza e protezione

informatica attualmente disponibili. Tali sistemi di sicurezza sono continuamente aggiornati e monitorati per garantire il livello di protezione adeguato.

I dati personali sono conservati in formato elettronico e vengono duplicati con frequenza giornaliera per premunirsi contro eventuali perdite o danneggiamenti.

Per i dati trattati con strumenti elettronici, inoltre, sono previste procedure di backup attraverso le quali Siena Ambiente S.p.A , effettua periodicamente una copia di tutti i dati presenti nel sistema. Il salvataggio dei dati avviene attraverso 3 procedure di backup:

- 1) backup su nastro;
- 2) backup su disco;
- 3) backup globale;
- 4) mirror fra le sedi di Siena e Poggibonsi

Backup su nastro

La cadenza è giornaliera (ora di esecuzione 21:00) esclusi il sabato e la domenica e viene effettuata su dieci unità nastro ognuna denominata con il giorno della settimana e suddivisi in due blocchi (settimana1 e settimana2). I nastri della settimana corrente sono conservati all'ufficio tecnico (sotto chiave), quelli della settimana non corrente in cassaforte all'amministrazione.

Elenco delle risorse incluse in questa procedura di backup sono incluse nei documenti che compongono l'ICT Security Policy

Backup su disco

E' eseguito sia presso la sede di Siena (server Sasint03) sia presso la sede di Poggibonsi (server Sapgnt02), in entrambi i casi tramite il software Robocopy, che produce un report che riporta l'esito del processo. La cadenza è giornaliera (ora di esecuzione 22,00) esclusi il sabato e la domenica.

Elenco delle risorse incluse in questa procedura di backup sono incluse nei documenti che compongono l'ICT Security Policy

Backup globale

Si effettua una volta alla settimana (il sabato alle 15) su disco FireWire rimovibile da 250 GB tramite Robocopy. Il disco viene conservato all'ufficio tecnico sotto chiave.

Elenco delle risorse incluse in questa procedura di backup:

- Tutti gli archivi e i database contenenti dati personali di cui sopra.

Mirror Siena-Poggibonsi e viceversa

Viene effettuato tramite Robocopy in modalità mirror (cioè vengono copiati solo i dati modificati rispetto all'esecuzione precedente). La cadenza è giornaliera (ora di esecuzione 23,00) esclusi il sabato e la domenica.

Segue l'elenco delle risorse incluse in questa procedura:

Siena→Poggibonsi:

- archivio dati ARC_SI con destinazione la cartella ARC_SI_BACKUP su Sapgnt02
- archivio del protocollo di Siena FTP con destinazione la cartella FTP_SI_BCK su Sapgnt02

Poggibonsi→Siena:

- archivio dati ARC_PG con destinazione la cartella ARCH_PG_BCK su Sasint03
- archivio del protocollo di Poggibonsi FTP con destinazione la cartella BCK_PG_VARIE su Sasint03

L'esito dei processi di backup è riportato in un file di report come nel caso del backup su disco.

I locali contenenti gli apparecchi che elaborano i dati sono protetti da intrusioni e l'accesso è riservato esclusivamente al personale tecnico incaricato della manutenzione degli elaboratori. L'esecuzione delle copie di backup di cui sopra garantisce, in caso di danneggiamento dei dati, tempi di ripristino minori di una giornata lavorativa nella maggior parte dei casi.

Si osserva, inoltre, **come i computer e** il server stesso risultano sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti, ecc.; il server è collegato ad un gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o interruzione di corrente elettrica.

Il ripristino dovrà essere effettuato in prima battuta dal backup su disco, in seconda battuta dal backup su nastro.

Il Backup Mirror e il Backup globale sono copie di sicurezza da utilizzare solo in situazione di grave emergenza (danneggiamento dei server, furti, gravi danni alle strutture aziendali, etc.) e

comunque solo se i due precedenti backup sono inutilizzabili. In particolare il backup globale è da considerarsi come ultima risorsa a cui attingere essendo il meno preciso di tutti (è svolto con frequenza settimanale).

In ogni caso il ripristino da backup **non** può essere intrapreso autonomamente dagli utenti; chi ne abbia bisogno deve rivolgersi al responsabile del Servizio Informatico.

E' adottato un sistema di accesso alle cartelle elettroniche contenenti dati personali protetto da password individuale che viene rinnovata ogni sei mesi. *(Punto 5 Disciplinare Tecnico)*

La parola chiave, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. *(Punto 5 Disciplinare Tecnico)*

La parola chiave non contiene riferimenti agevolmente riconducibili all'incaricato. *(Punto 5 Disciplinare Tecnico)*

La parola chiave modificata viene modificata dall'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi. *(Punto 5 Disciplinare Tecnico)*

In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave viene modificata almeno ogni tre mesi. *(Punto 5 Disciplinare Tecnico)*

Gli incaricati hanno adottato le necessarie cautele per assicurare la segretezza della parola chiave e custodiscono diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetico, tessere magnetiche, ecc..).

Gli incaricati dei trattamenti personali hanno disposizione di non divulgare la loro parola chiave.

In merito a messaggi e-mail inviati a più destinatari, quale destinatario dovrà essere indicata la nostra società con il nostro indirizzo e-mail, ed in CCN i destinatari (che in tal modo non possono individuare gli indirizzi e-mail degli altri interessati, attraverso le funzioni di proprietà).

7 Trattamento dei dati con l'ausilio di supporto cartaceo

I supporti cartacei sono raccolti in schedari a loro volta custoditi in armadi.

Gli archivi del personale e contenenti documenti amministrativi (fiscale, previdenziale, contributiva, retributiva, ecc.) sono localizzati nell'ufficio amministrativo ove in appositi armadi vengono archiviati i supporti cartacei di comune e continuo utilizzo da parte del solo personale dell'ufficio amministrativo.

Per ogni archivio i responsabili della sicurezza dei dati personali hanno definito l'elenco degli incaricati autorizzati ad accedervi e le istruzioni tese a garantire un controllo costante nell'accesso degli archivi, ovvero:

- 1) Gli incaricati che trattano atti o documenti personali sono tenuti a conservarli e restituirli al termine delle operazioni;
- 2) È vietato effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal responsabile della sicurezza dei dati personali, di stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- 3) È vietato sottrarre, cancellare, distruggere senza l'autorizzazione del responsabile della sicurezza dei dati personali, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- 4) È vietato consegnare a persone non autorizzate dal responsabile della sicurezza dei dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

Relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nei seguenti:

- qualsiasi documento che i Sig.ri Clienti consegnino alla società va inserito, quando personale, in apposite cartelline non trasparenti;
- qualsiasi documento che la società consegni ai Sig.ri Clienti va inserito in apposite buste o cartelline non trasparenti.

Le rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contiene alcun dato (praticamente il primo foglio funge da copertina).

Le copie dei telefax inviati mediante apparecchio tradizionale sono riconsegnate a colui che ha eseguito o fatto eseguire la trasmissione, avendo cura di porre al primo foglio il rapporto di trasmissione formato A4 che viene stampato dal fax , con di seguito i fogli contenenti il messaggio. Eventuali copie di documenti, di scritti, di appunti, di tabulati prova ecc. sono distrutte manualmente.

Il consenso/informativa al trattamento dei dati personali, fatto sottoscrivere a ciascun Cliente, prevede che copie ed originali della documentazione dell'interessato possano essere consegnate al coniuge o a conviventi, od a figli, o personale dipendente del Cliente e che detta consultazione avrà validità sino a revoca da effettuarsi con lettera raccomandata a.r. da inviare alla società e che tale revoca avrà effetto dal giorno successivo a quello del ricevimento

Si evidenzia che il presente DPS scaturisce da una prima analisi di valutazione dei rischi e che è previsto l'aggiornamento dello stesso nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro.

8 Descrizione del sistema informatico

8.1 Server e sistemi multi utenti:

Attualmente sono presenti n° 8 server:

1 COMPAQ PROLIANT ML 350 WIN 2000 SERVER CONFIGURAZIONE TERMINAL SERVER.

2 COMPAQ PROLIANT ML 350 WIN 2000 SERVER CONFIGURAZIONE TERMINAL SERVER.

3 COMPAQ PROLIANT ML 350 WIN 2000 SERVER CONFIGURAZIONE DATABASE SERVER.

4 COMPAQ PROLIANT DL 360 WIN 2000 SERVER CONFIGURAZIONE TERMINAL SERVER.

5 HP NETSERVER WIN 2000 SERVER CONFIGURAZIONE DOMAIN CONTROLLER.

6 HP NETSERVER WIN 2000 SERVER CONFIGURAZIONE DOMAIN E FILE SERVER

7 HP NETSERVER WIN 2000 SERVER CONFIGURAZIONE DOMAIN E FILE SERVER

8 COMPAQ PROLIANT DL 380 WIN 2000 IN CONFIGURAZIONE DATABASE SERVER

8.2 Reti locali ed altri sistemi di collegamento terminali.

È presente rete locale LAN su TCP/IP operante su cablaggio di rete di tipo ethernet. Sono inoltre presenti i seguenti collegamenti con sedi periferiche:

- uffici Poggibonsi
- impianto di Termovalorizzazione in loc. Fosci
- deposito mezzi presso magazzino comunale di Poggibonsi
- impianto di depurazione di Chiusi
- uffici di Siena, via Cerchiaia

Per la descrizione degli apparati utilizzati per i collegamenti con le sedi periferiche vedere la sezione Dispositivi di connessione verso l'esterno.

8.3 Personal computer

Collegati alla rete, ad esclusione del server, esistono n° 50 personal Computer prevalentemente di marca Compaq e HP.

8.4 Personal Computer portatili

Son presenti in azienda n° 10 personal computer portatili:

- Compaq Evo in dotazione al responsabile della Sicurezza sul Lavoro
- Toshiba Satellite in dotazione al responsabile del settore Raccolta
- Acer Travelmate in dotazione al personale del servizio Raccolta

I rimanenti portatili (prevalentemente di marca Acer) sono in dotazione al personale addetto all'ufficio e agli sportelli della TIA. L'accesso ai portatili è protetto da password e comunque sul disco fisso non è memorizzata nessuna informazione personale o sensibile.

Tutti i portatili sono dotati di scheda per l'accesso alla rete.

8.5 Unità di accesso per gli operatori.

Tutti i PC possono essere accessibili dagli altri PC solo attraverso reti non disponibili al pubblico.

8.6 Dispositivi di connessione verso l'esterno

Sono presenti Router Cisco 1600, Firewall Watchguard SOHO e Firewall Cisco Pix.

I Router Cisco e i Firewall sono utilizzati per i collegamenti con le sedi periferiche realizzati mediante linee Telecom ADSL e HDSL. Inoltre il collegamento tra gli uffici di Siena e di Poggibonsi è realizzato mediante collegamento punto-punto in fibra ottica, realizzato dal provider Terre Cabbate. Lo stesso provider fornisce anche l'accesso web sullo stesso supporto. La configurazione dei collegamenti è di tipo tunnel VPN basato su algoritmi rendendo di fatto la WAN aziendale chiusa al pubblico.

È presente inoltre un Proxy Server per la regolamentazione degli accessi alle pagine web. Tale regolamentazione si basa su liste di pagine vietate stilate a livello internazionale e continuamente aggiornate.

8.7 Collegamenti del sistema a dispositivi di acquisizione dati

Sono presenti n° 3 rilevatori presenze, uno collegato in modalità punto-punto con cavo seriale al server dedicato alla gestione della base dati di gestione delle presenze, gli altri due tramite interfaccia ethernet alla rete aziendale ma comunque raggiungibili solo dalle postazioni

dell'ufficio personale, che sono le uniche fornita del software in grado di acquisire i dati registrati dai rilevatori.

Tab. 8. Criteri e procedure per il ripristino e salvataggio della disponibilità dei dati

RIPRISTINO		
Banca/data base/ archivio dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
ARC-SI; Q; ZETA FAX; FTP SIENA;	Back Up - giornaliero	La prima volta che un nuovo sistema di back up viene installato si fa la prova di ripristino; successivamente all'occorrenza.
DATI CONTABILITÀ; WINSMART; SUPERGULP; EXCHANGE; NAVISION; INFOR; DATI PRESENZE; OFA	Back Up - giornaliero	
REGISTRO E STATO DEL SISTEMA DEI SERVER	Back Up - giornaliero	
ARC-PG; P; FTP;	Back Up - giornaliero	

SALVATAGGIO			
Banca/data base/ archivio dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio
ARC-SI; Q; ZETA FAX; FTP SIENA;	Back Up - giornaliero	Sede impresa ufficio	Sistema informatico
DATI CONTABILITÀ; WINSMART; SUPERGULP; EXCHANGE; NAVISION; INFOR; DATI PRESENZE; OFA	Back Up - giornaliero	Sede impresa ufficio	
REGISTRO E STATO DEL SISTEMA DEI SERVER	Back Up - giornaliero	Sede impresa ufficio	
ARC-PG; P; FTP;	Back Up - giornaliero	Ufficio Poggibonsi.	

Gli incaricati del trattamento sono stati debitamente informati circa il contenuto del presente documento e sono obbligati ad uniformarsi allo stesso mentre il responsabile del trattamento è obbligato a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati

Una copia verrà consegnata ai responsabili dei determinati trattamenti di dati appositamente nominati.

Il presente documento è stato ulteriormente illustrato nel corso di una riunione, tenutasi in orario di lavoro, alla quale hanno partecipato il titolare, i responsabili e gli incaricati del trattamento, nel rispetto delle disposizioni di cui al D. Lgs. 196/2003 nel disciplinare Tecnico in materia di misure minime di Sicurezza che prevede un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni, nonostante la predetta norma riguardi esclusivamente gli elaborati accessibili mediante una rete di telecomunicazioni disponibili al pubblico che non sono in possesso della società.

Il presente documento è stato approvato dal Consiglio di Amministrazione in data 27 ottobre 2005 , e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.

Allegato

Disciplinare Tecnico in materia di misure minime di Sicurezza (Artt. da 33 a 36 del Codice)

Trattamento con strumenti elettronici

Modalità tecniche da adottare a cura del Titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici.

Sistema di autenticazione informatica

1. Il trattamento dei dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da questo ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente

all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno

semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare del trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. L'elenco dei trattamenti di dati personali;

19.2. La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. L'analisi dei rischi che incombono sui dati;

19.4. Le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. La previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. Per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti

non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamento senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Definizioni (Art. 4 D. Lgs 196/2003)

Ai fini della migliore comprensione del DPS si riportano qui di seguito le definizioni di cui all'art. 4 del Codice.

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 dati.

DATO PERSONALE

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificato o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI

Dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI

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;

DATI GIUDIZIARI

Dati personali idonei a rivelare provvedimenti di cui all'art. 3 comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14-11-2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di Procedura Penale.

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 dei dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

RESPONSABILE

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.

INCARICATI

Le persone fisiche autorizzate dal titolare o dal responsabile a compiere operazioni di trattamento di trattamento dal titolare o dal responsabile.

INTERESSATO

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

COMUNICAZIONE

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

DIFFUSIONE

Il dare conoscenza di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

DATO ANONIMO

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

BLOCCO

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

BANCA DATI

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

COMUNICAZIONE ELETTRONICA

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

CHIAMATA

La connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale.

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 segnali, le reti televisive via cavo, indipendente dal tipo di informazione trasportato.

RETE PUBBLICA DI COMUNICAZIONE

Una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibile al pubblico.

SERVIZIO DI COMUNICAZIONE ELETTRONICA

I servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'art. 2, lettera c) della direttiva 2002/21/CE del 7 marzo 2002, del Parlamento Europeo e del Consiglio.

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.

UTENTE

Qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

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.

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.

SERVIZIO A VALORE AGGIUNTO

Il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione.

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.

MISURE MINIME

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione in relazione ai rischi previsti nell'art. 31.

STRUMENTI ELETTRONICI

Gli elaborati, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

AUTENTICAZIONE INFORMATICA

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

CREDENZIALI DI AUTENTICAZIONE

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

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.

PROFILO DI AUTORIZZAZIONE

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

SISTEMA DI AUTORIZZAZIONE

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

SCOPI STORICI

Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato

SCOPI STATISTICI

Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici.

SCOPI SCIENTIFICI

Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.