

Comune di Verdellino



(Provincia di Bergamo)

Piazza don Martinelli, 1 - 24040 Verdellino
cod.fisc./p.IVA 00321950164 - tel. 0354182811 – fax. 0354182899
E-Mail: info@comune.verdellino.bg.it - PEC: comune.verdellino@registerpec.it
sito internet: www.comune.verdellino.bg.it

DOCUMENTO PROGRAMMATICO

SULLA SICUREZZA DEI DATI

**REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1,
LETTERA G) DEL DLGS 196/2003, E DEL DISCIPLINARE TECNICO
ALLEGATO AL MEDESIMO DECRETO SUB B)**

AGGIORNAMENTO ANNO 2010

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

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 dal **Comune di Verdellino con sede in Piazza Don Martinelli, 1 24040 VERDELLINO (BG) – Codice fiscale 00321950164** (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:

- Martinelli Gianfranco, istruttore direttivo.

=====

Conformemente a quanto prescrive il punto 19. del Disciplinare tecnico, allegato sub b) al D.lgs 196/2003, nel presente documento si forniscono idonee informazioni riguardanti individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
 - la individuazione dei tipi di dati personali trattati
 - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
 - la elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi degli incaricati del trattamento
3. l'analisi dei rischi che incombono sui dati
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento
6. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
7. le procedure da seguire per il controllo sullo stato della sicurezza
8. dichiarazioni d'impegno e firma.

Indice:

1	L'elenco dei trattamenti dei dati personali	Pag. 3
	1 Tipologie di dati trattati	
	2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti	
	3 La mappa dei trattamenti effettuati	
2	Mansionario privacy ed interventi formativi degli incaricati	Pag. 12
3	Analisi dei rischi che incombono sui dati	Pag. 17
4	Misure atte a garantire l'integrità e la disponibilità dei dati	Pag. 20
	1 La protezione di aree e locali	
	2 La custodia e l'archiviazione di atti, documenti e supporti	
	3 Le misure logiche di sicurezza	
5	Criteri e modalità di ripristino dei dati	Pag. 29
6	L'affidamento di dati personali all'esterno	Pag. 31
7	Controllo generale sullo stato della sicurezza	Pag. 34
8	Dichiarazioni d'impegno e firma	Pag. 35

1. L'elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si è proceduto come segue:

- Si individuano i tipi di dati personali trattati, in base alla loro natura, alla categoria di soggetti cui essi si riferiscono e alla finalità.
- si descrivono le aree, i locali e gli strumenti con i quali si effettuano i trattamenti.
- si elabora la mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti.

1.1 Tipologie di dati trattati

Nelle tabelle allegate sono individuati e distinti per ciascun settore, i trattamenti effettuati, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, (nonché degli strumenti elettronici impiegati).

Al fine della stesura della mappa dei trattamenti effettuati e della redazione del mansionario i dati trattati dal Titolare si riassumono in modo esaustivo come segue:

Dati comuni relativi a clienti /cittadini / dipendenti.

Dati comuni relativi a fornitori.

Dati comuni relativi ad altri soggetti.

Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali.

Dati di natura giudiziaria relativi a clienti, fornitori, cittadini, dipendenti e ad altri soggetti.

Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile.

Dati di natura sensibile relativi a clienti / fornitori / utenti / cittadini.

Dati idonei a rivelare lo stato di salute e/o la vita sessuale dei cittadini.

Dati idonei a rivelare l'affezione da virus HIV.

Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti.

Dati biometrici relativi al personale e ad altri soggetti. *

***Attualmente non è installato alcun sistema elettronico in grado di acquisire questi dati, ma con molta probabilità potrebbe essere installato nel prossimo futuro. In vista dei prossimi aggiornamenti annuali del documento le tabelle di analisi prevedono già questi tipi di dati anche se non trattati.**

1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Il trattamento dei dati personali avviene nei **seguenti edifici**:

Palazzina del Municipio

E' situata in Piazza don Martinelli, 1 in zona centrale del comune di Verdellino (BG). La palazzina si sviluppa su tre piani più un piano interrato. Esiste un'area comune (identificata come area scale e ascensore) che comunica con tutti i 4 livelli ed è accessibile dalla porta dell'entrata principale (chiudibile a chiave e dotata di sbarre anti intrusione) all'interno della quale non viene effettuato alcun trattamento e archiviazione di dati. Le zone di trattamento e archiviazione dati sono state identificate perchè isolabili dalle altre in quanto provviste di porte chiudibili a chiave o con porte in vetro antisfondamento motorizzate, attivabili tramite inserimento codice segreto a 4 cifre e quindi eventualmente configurabili (ad esempio fuori dall'orario di lavoro come zone ad accesso controllato). Tali zone sono riassunte e classificate in questa lista:

Piano interrato:

- Locale archivio

Piano Terra:

- Ufficio Servizi Sociali ed Istruzione Pubblica
- Ufficio Servizi Sociali
- Ufficio Anagrafe

Primo piano:

- Saletta quadro di rete
- Ufficio open space Ragioneria/Segreteria/Protocollo/Urp/Messo/Servers .
- Ufficio Segretario.
- Ufficio Sindaco.
- Sala riunioni.

Secondo piano:

- Area Sala consigliare.
- Ufficio tecnico.

Sede della Biblioteca Comunale

E' situato in Via Principe Amedeo, 53 in zona centrale del comune di Verdellino (BG). La sede si sviluppa su 2 livelli comunicanti tra di loro tramite un'ampia scala esterna. I due livelli sono dei locali open space che definiscono di fatto due aree ben distinte ognuna dotata di porte di accesso chiudibili a chiave.

Sede dell'Asilo Nido

E' situato in Via Rodari, 8 in zona centrale del Comune di Verdellino (BG). La sede si sviluppa su un unico piano. L'unica area destinata al trattamento e all'archivio dei dati è un locale dotato di un'unica porta di accesso chiudibile a chiave con all'interno un armadio anch'esso chiudibile a chiave.

Sede del Comando della Polizia Locale

E' situato in Via Verdi, 13 in zona centrale del comune di Verdellino (BG). La sede è al piano terra di una palazzina ed ha un accesso indipendente. Inoltre è presente al piano semi-interrato un altro locale destinato ad autorimessa. Tutte gli accessi e le finestre sono protette da inferriate. L'area destinata al trattamento e all'archivio dei dati sono i locali al piano terra che sono ulteriormente isolati dall'area accessibile al pubblico da un divisorio dotato di porta chiudibile a chiave vengono classificati come unico ufficio, pur disponendo di porte con chiave. All'interno dell'area sono presenti armadi anch'essi chiudibili a chiave e una cassaforte. Essendo installato in modo fisso un personal computer all'interno delle due autovetture in dotazione alla Polizia locale (personal computer dotato di supporto di archiviazione dati non rimovibile), le autovetture vengono assimilate ad area di trattamento dati.

Tali zone sono riassunte e classificate in questa lista:

Piano Terra:

- Ufficio Polizia Locale

Autovettura:

- Alfa 159 targata DA554NZ
- Ford Mondeo targata CM330PE

Il trattamento dei dati personali avviene con i **seguenti strumenti**:

A – Schedari ed altri supporti cartacei

I supporti cartacei, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, come segue:

- Ogni struttura organizzativa dispone nei propri uffici / zone di trattamento armadi dotati di chiusura a chiave da destinare a quelle banche dati di cui sono incaricate che contengono dati personali (sensibili e giudiziari). Solo nel caso che la banca dati contenga esclusivamente dati (comuni) vengono utilizzati eventuali parti di armadi non chiudibili a chiave.
- E' presente inoltre una zona archivio al piano semi interrato sempre chiusa a chiave dove sono contenuti in armadi anch'essi chiusi a chiave i dati degli anni precedenti, classificati per banche dati e per anno.

B – Elaboratori non in rete

Il titolare dispone di un solo pc non in rete, utilizzato come postazione lavoro nell'area di trattamento identificata come Asilo Nido.

C – Elaboratori in rete privata

Il titolare non dispone di pc in rete privata.

D – Elaboratori in rete pubblica

PALAZZINA MUNICIPIO

Numero 27 postazioni fisse, così suddivise e dislocate come segue:

- 01 Elaboratore con funzioni di Server al primo piano nella palazzina Municipio, nell'area classificata come saletta adibita a centraline elettrica, telefonica e impianti informatici.
- 01 Elaboratore con funzioni di Server di posta e di Backup di rete al primo piano nella palazzina Municipio, nell'area classificata come saletta adibita a centraline elettrica, telefonica e impianti informatici.
- 01 Elaboratore con funzioni di Firewall al primo nella palazzina Municipio nell'area classificata come saletta adibita a centraline elettrica, telefonica e impianti informatici.
- 01 Elaboratore con funzioni di postazione lavoro al primo piano nella palazzina Municipio nell'area classificata come Ufficio Segretario.
- 09 Elaboratori con funzioni di postazione lavoro al primo piano nella palazzina Municipio nell'area classificata come Ufficio open space Ragioneria/Segreteria/Protocollo/Urp/Messo/Servers.
- 07 Elaboratori con funzioni di postazione lavoro al secondo piano nella palazzina Municipio nell'area classificata come Ufficio Tecnico.
- 03 Elaboratori con funzioni di postazione lavoro al piano terra nella palazzina Municipio come Ufficio Anagrafe.
- 01 Elaboratore con funzioni di porta d'accesso per le applicazioni legate alla C.I.E (Carta d'identità elettronica) al piano terra nella palazzina Municipio come Ufficio Anagrafe.
- 01 Elaboratore con funzioni di postazione lavoro al piano terra nella palazzina Municipio nell'area classificata come Ufficio Servizi Sociali.
- 02 Elaboratori con funzioni di postazione lavoro al piano terra nella palazzina Municipio nell'area come Ufficio Servizi Sociali ed Istruzione Pubblica.

Numero 02 computer portatili così suddivise e dislocate come segue:

- 01 Computer portatile con funzioni di postazione lavoro assegnato all'Ufficio Tecnico.
- 01 Computer portatile con funzioni di postazione lavoro assegnato al Sindaco.

Numero Scanner e Stampanti, così suddivise e dislocate come segue:

- 22 Stampanti dislocate nei vari uffici per le relative esigenze lavorative delle strutture organizzative.
- 08 Scanners dislocati nei vari uffici per le relative esigenze lavorative delle strutture organizzative.
- 01 Scanner dedicato al protocollo informatico.

Numero 06 fotocopiatrici, così suddivise e dislocate come segue:

- Fotocopiatrici dislocate per le esigenze lavorative delle strutture organizzative (1 Ufficio Servizi Sociali, 1 Ufficio Anagrafe, 1 Ufficio open space Ragioneria /Segreteria/ Protocollo / Urp / Messo / Servers, 2 Ufficio Tecnico, 1 archivio).

Altri strumenti elettronici quali router, switches, dispositivi di backup etc. dislocati nell'area classificata come saletta adibita a centraline elettrica, telefonica e impianti informatici.

BIBLIOTECA

Numero 10 postazioni fisse, così suddivise e dislocate come segue:

- 01 elaboratore (mini p.c.) con funzioni di Firewall nel locale al piano terra della Biblioteca.
- 04 elaboratori con funzioni di postazione accesso internet e utilizzo multimediale riservato al pubblico al piano terra della Biblioteca.
- 02 elaboratori con funzioni di postazione accesso al sistema Opac Provinciale, al piano terra e al primo piano.
- 03 elaboratori con funzioni di postazione lavoro di cui 02 al piano terra e 01 al primo piano della Biblioteca.

Numero 01 computer portatili, così suddivise e dislocate come segue:

- 01 computer portatile, dato in dotazione alla Biblioteca.

Numero 02 Stampanti, 01 fotocopiatore, 01 scanner per le esigenze della Biblioteca.

ASILO NIDO

Numero 01 fotocopiatrice per le esigenze dell'Asilo Nido.

Numero 01 elaboratore, non in rete, per le esigenze del servizio.

Numero 01 stampante per le esigenze del servizio.

COMANDO POLIZIA LOCALE

Numero 7 postazioni fisse, così suddivise e dislocate come segue:

- 04 elaboratore con funzioni di postazione lavoro nell'area classificata come ufficio Polizia Locale.
- 03 elaboratore con funzioni di registrazione dati (n. 2 x immagini – n.1 x suoni) provenienti dalle telecamere sempre nell'area di trattamento dati classificata come ufficio Polizia Locale.

Numero 02 computer portatili, così suddivise e dislocate come segue:

- 01 computer portatile installato all'interno dell'autovettura classificata come area di trattamento dati Ford Mondeo targata CM330PE.
- 01 computer portatile però installato in modo fisso all'interno dell'autovettura classificata come area di trattamento dati Alfa 159 targata DA554NZ.
- Numero 03 Stampanti, 01 scanner, 01 fax e 01 fotocopiatrici dislocati nell'area classificata come ufficio Polizia Locale.

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti

Sono state installate nel territorio Comunale n. 19 telecamere qui elencate in dettaglio:

POSIZIONE	TIPO	DITTA	MARCA	MODELLO	DESCRIZIONE
Via / Piazza	Fissa/ brandeggiabile	FGS – Azzano S. Paolo			area videosorvegliata
Corso Europa	brandeggiabile	idem	BTE	HID2404SSE11P	Piazza Affari (*)
Corso Europa	fissa	idem	BTE	HCB-F90N	Area di sosta via C. Porta, 37 (*)
Via C. Porta	brandeggiabile	idem	BTE	HID2404SSE11P	Via C. Porta (*)
Corso Asia	fissa	idem	BTE	HCB-F90N	Piazza Affari (*)
Via Oleandri	brandeggiabile	idem	BTE	HID2404SSE11P	Via Oleandri (*)
Corso Asia	fissa	idem	BTE	HCB-F90N	Via Oleandri – Corso Asia (rotatoria) (*)
Corso Italia	fissa	idem	BTE	HCB-F90N	Corso Italia – Piazzola ecologica
Corso Italia	fissa	idem	BTE	HCB-F90N	Corso Italia – Piazzola ecologica
Corso Italia	fissa	idem	BTE	HCB-F90N	Corso Italia – Piazzola ecologica
Via C. Alvaro	fissa	idem	AXIS	221	Area di sosta via C. Alvaro
Via Morletta	fissa	idem	AXIS	221	Ingresso 1 area di sosta via Morletta
Via Morletta	fissa	idem	AXIS	221	Ingresso 2 area di sosta via Morletta
Via Morletta	fissa	idem	AXIS	221	Ingresso 3 area di sosta via Morletta
Via Morletta	brandeggiabile	idem	AXIS	213	Area di sosta via Morletta
Via Morletta	brandeggiabile	idem	AXIS	213	Area di sosta Stazione FS ed accesso pedonale all'area di sosta via Morletta (*)
Via Verdi	fissa	idem	AXIS	221	Ingresso Comando Polizia Locale
Via Verdi	fissa	idem	AXIS	221	Area di sosta Comando Polizia Locale
Via Verdi	brandeggiabile	idem	AXIS	213	Via Verdi e Piazzale Sabin
Alfa 159	brandeggiabile	idem	AXIS	213	Visuale mobile sul territorio comunale

(*) – Telecamere collegate anche con la Stazione Carabinieri di Zingonia per la relativa visione.

E' inoltre installato un sistema di registrazione solo audio delle sedute del Consiglio Comunale. Nel regolamento per l'organizzazione e il funzionamento del Consiglio Comunale, modificato con delibera di consiglio n. 31 del 06/09/2005, all'art. 23 comma 4. si è specificato l'uso e la destinazione di tale apparecchiatura. I relativi CD sono archiviati in armadietto chiuso a chiave nel Ufficio open space Ragioneria/Segreteria/Protocollo/Urp/Messo/Servers.

F – Altri strumenti (es. basati su dati biometrici,)

Attualmente non è installato alcun dispositivo.

Dall'analisi di quanto descritto precedentemente otteniamo questa tabella dove la **X** significa che un determinato strumento di archiviazione è presente:

AREE																
Locale archivio	X	X														
Ufficio Polizia Locale			X		X						X				X	
Alfa 159 targata DA554NZ		X				X									X	
Ford Mondeo targata CM330PE		X				X										
Ufficio Servizi Sociali ed Istruzione Pubblica	X	X									X					
Ufficio Servizi Sociali	X	X									X					
Ufficio Anagrafe	X	X									X					
Saletta adibita a centraline elettrica, telefonica e impianti informatici												X				
Ufficio open space Ragioneria, Segreteria, Protocollo, Urp, Messo, Servers	X	X									X					
Ufficio Segretario.	X	X									X					
Ufficio Sindaco	X	X											X			
Sala riunioni	X	X														
Area Sala consigliere																X
Ufficio tecnico	X	X									X		X			
Biblioteca piano terra	X	X									X					
Biblioteca primo piano	X	X									X					
Locale Asilo nido	X	X		X												
	A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3	E	F		
	TIPI DI STRUMENTI															

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:

- **A1** quelli custoditi in un'area ad accesso non controllato
- **A2** quelli custoditi in un'area ad accesso non controllato in armadio chiuso a chiave
- **A3** quelli custoditi in un'area ad accesso controllato

B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:

- **B1** quelli localizzati in un'area ad accesso non controllato
- **B2** quelli localizzati in un'area ad accesso controllato
- **B3** quelli portatili o altri dispositivi mobili

C – Elaboratori in rete privata

- **C1** quelli localizzati in un'area ad accesso non controllato
- **C2** quelli localizzati in un'area ad accesso controllato
- **C3** quelli portatili o altri dispositivi mobili

D – Elaboratori in rete pubblica

- **D1** quelli localizzati in un'area ad accesso non controllato
- **D2** quelli localizzati in un'area ad accesso controllato
- **D3** quelli portatili o altri dispositivi mobili

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti.

F – Altri strumenti (es. basati su dati biometrici).

1.3 La mappa dei trattamenti effettuati

Incrociando le coordinate di cui ai due paragrafi precedenti, si ottiene la mappa dei trattamenti di dati personali effettuati dal Titolare. Il simbolo **X** apposto nella casella di incrocio, significa che determinati tipi di dati sono trattati con determinati strumenti. Nella tabella di incrocio, si appone un simbolo identificativo di ciascun trattamento, che sta tra l'altro a significare che determinati tipi di dati sono trattati con determinati strumenti.

TIPI DI TRATTAMENTI														
Dati comuni relativi a clienti /cittadini / dipendenti.	X			X							X		X	
Dati comuni relativi a fornitori.	X			X							X		X	
Dati comuni relativi ad altri soggetti.	X			X							X		X	
Dati biometrici relativi al personale e ad altri soggetti.*														
Dati idonei a rilevare la posizione di persone ed oggetti.														X
Dati relativi allo svolgimento di attività economiche...	X	X									X			
Dati di natura giudiziaria relativi a clienti, fornitori, cittadini..		X									X			
Dati sensibili al personale, nonché ai candidati per diventarlo		X									X			
Dati di natura sensibile relativi a clienti/fornitori/cittadini.		X									X			
Dati idonei a rivelare lo stato di salute e/o la vita sessuale.		X									X			
Dati idonei a rivelare l'affezione da virus HIV.		X									X			
* attualmente non trattati	A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3	E	F
	TIPI DI STRUMENTI													

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:

- **A1** quelli custoditi in un'area ad accesso non controllato
- **A2** quelli custoditi in un'area ad accesso non controllato in armadio chiuso a chiave
- **A3** quelli custoditi in un'area ad accesso controllato

B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:

- **B1** quelli localizzati in un'area ad accesso non controllato
- **B2** quelli localizzati in un'area ad accesso controllato
- **B3** quelli portatili o altri dispositivi mobili

C – Elaboratori in rete privata

- **C1** quelli localizzati in un'area ad accesso non controllato
- **C2** quelli localizzati in un'area ad accesso controllato
- **C3** quelli portatili o altri dispositivi mobili

D – Elaboratori in rete pubblica

- **D1** quelli localizzati in un'area ad accesso non controllato
- **D2** quelli localizzati in un'area ad accesso controllato
- **D3** quelli portatili o altri dispositivi mobili

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti.

F – Altri strumenti (es. basati su dati biometrici).

Da una prima lettura della mappa, si evince che:

- Tutti i dati indifferentemente dalla natura vengono trattati e/o archiviati in aree che non sono ad accesso controllato. Nessuna delle aree di trattamento è considerata in questa sede ad accesso controllato in quanto non esiste nessun dispositivo elettronico che durante l'orario di lavoro possa identificare esattamente l'identità, e memorizzare l'orario di accesso e di uscita di chi accede ad una determinata area. In ogni caso si precisa che nel presente mansionario sono fornite agli incaricati dei trattamenti tutte le indicazioni per una corretta gestione dei dati trattati e della loro custodia, nonché per la vigilanza e il controllo delle aree di trattamento in cui direttamente operano.
- Tutti i dati sensibili e giudiziari vengono archiviati in armadi chiusi a chiave.
- Tutti i dati indifferentemente dalla natura vengono trattati e/o archiviati sia con strumenti diversi da quelli elettronici (sostanzialmente archivi cartacei) che con quelli elettronici.
- La quasi totalità dei dati è trattata per quanto riguarda gli strumenti elettronici è trattata con pc in rete pubblica.
- I dati relativi allo stato di salute / la vita sessuale di cittadini vengono in una zona senza accesso controllato con in armadi chiusi a chiave e trattati con strumenti elettronici collegati in rete pubblica.
- E' presente un sistema di videosorveglianza dotato di 19 telecamere e un sistema di registrazione solo audio nella sala consigliare. Le registrazioni sono archiviate nelle modalità e per i tempi previsti dal garante in un personal computer presente all'interno del Comando di Polizia Locale e in quello presente all'interno dell'autovettura Alfa 159 targata DA554NZ. I CD audio della sala consigliare sono archiviati in armadietto chiuso a chiave nel Ufficio open space Ragioneria/Segreteria/Protocollo/Urp/Messo/Servers.

Queste considerazioni saranno oggetto di analisi nei capitoli successivi.

2. Mansionario privacy ed interventi formativi degli incaricati

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

SETTORE / SERVIZIO	NOMINATIVO	PROVVEDIMENTO DI NOMINA
Responsabile Amministrativo Privacy	Martinelli Gianfranco	Atto di nomina del Sindaco in data 03/09/2004 – prot. n° 13.993 -
Responsabile Informatico Privacy – Amministratore del sistema	Rosa Pierangela	Atto di nomina del Sindaco in data 03/09/2004 – prot. n° 13.995 -
Responsabile Settore Servizi Amministrativi	Pansera Antonia	Atto di nomina del Sindaco in data 12/12/2008 – prot. n° 14.127 -
Responsabile Settore Lavori Pubblici	Camizzi Mario	Atto di nomina del Sindaco in data 12/12/2008 – prot. n° 14.127 -
Responsabile Settore Servizi Sociali	Carera Angela	Atto di nomina del Sindaco in data 12/12/2008 – prot. n° 14.127 -
Responsabile Settore Servizi Finanziari	Teoldi Silvia	Atto di nomina del Sindaco in data 12/12/2008 – prot. n° 14.127 -
Responsabile Settore Urbanistica e Ambiente	Guerini Giovanna	Atto di nomina del Sindaco in data 12/12/2008 – prot. n° 14.127 -
Responsabile Settore Polizia Locale	Colombo Angelo	Atto di nomina del Sindaco in data 12/12/2008 – prot. n° 14.127 -
Responsabile Servizio Commercio e Pubblici Esercizi - Istruzione e Cultura	Brolis Dr. Angelo	Atto di nomina del Sindaco in data 26/03/2010 – prot. n° 3.880 -

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante documentata preposizione di ogni persona ad una unità, per la quale sia stato previamente individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima.

Di seguito si riporta l'elenco degli **INCARICATI AL TRATTAMENTO DEI DATI INTERNI ALL'ENTE**, con la specifica del provvedimento di nomina e dei servizi per i quali sono stati autorizzati ai trattamenti dei dati.

SETTORE	RESPONSABILE DI SETTORE	Servizi	Incaricati del trattamento	
			Nome dell'incaricato	Provvedimento di nomina
N° 1 - AMMINISTRAZIONE GENERALE	Pansera Antonia	Protocollo - Archivio -Notifiche	Nisoli Enrico	Nomina del resp. settore del 22/12/08 - prot. 14567-
			Nozza Fiorenza	Nomina del resp. settore del 22/12/08 - prot. 14567-
			Martinelli Gianfranco	Nomina del resp. settore del 22/12/08 - prot. 14567-
		Organi istituzionali - Urp - contratti	Martinelli Gianfranco	Nomina del resp. settore del 22/12/08 - prot. 14567-
		Segreteria - C.ED. - Personale - Assicurazioni - Conv. att. Soc. utili - Sponsorizz.	Rosa Pierangela	Nomina del resp. settore del 22/12/08 - prot. 14567-
		Servizio anagrafe, stato civile, elettorale, leva, toponomastica	Nozza Carolina	Nomina del resp. settore del 22/12/08 - prot. 14567-
			Vavassori Cristina	Nomina del resp. settore del 22/12/08 - prot. 14567-
			Grasselli Angela Grazia	Nomina del resp. settore del 22/12/08 - prot. 14567-
N° 2 - LAVORI PUBBLICI E PATRIMONIO	Camizzi Mario	Lavori pubblici - cosap - gestione patrimonio comunale - sport	Rondelli Simone	Nomina del resp. settore del 22/12/08 - prot. 14568-
			Zanchi Bruna	Nomina del resp. settore del 22/12/08 - prot. 14568-
N° 3 - SERVIZI SOCIALI	Carera Angela	Asilo Nido	Mauro Tiziana	Nomina del resp. settore del 22/12/08 - prot. 14569-
			Manzoni Irene	Nomina del resp. settore del 22/12/08 - prot. 14569-
			Foppa Lucia	Nomina del resp. settore del 22/12/08 - prot. 14569-
		Servi sociali	Gioia Cristina	Nomina del resp. settore del 22/12/08 - prot. 14569-
N° 4 - SERVIZI FINANZIARI	Teoldi Silvia	Ragioneria e programmazione - Tributi e Provveditorato	Duzioni Wilma	Nomina del resp. settore del 22/12/08 - prot. 14570-
			Delcarro Angelo	Nomina del resp. settore del 22/12/08 - prot. 14570-
			Ferrari Katuscia	Nomina del resp. settore del 22/12/08 - prot. 14570-

SETTORE	RESPONSABILE DI SETTORE	Servizi	Incaricati del trattamento	
			Nome dell'incaricato	Provvedimento di nomina
N° 5 - URBANISTICA ED ECOLOGIA	Guerini Giovanna	Urbanistica - Edilia res. Pubbl. - Tutela ambientale - Aut. att. produtt. - Distributori Carburanti - servizi sovra-comun. territorio	Guerreri Marco	Nomina del resp. settore del 22/12/08 - prot. 14571-
N° 6 - POLIZIA LOCALE E PROTEZIONE CIVILE	Colombo Angelo	Polizia Locale e Protezione Civile	Blandini Nicolò	Nomina del resp. settore del 22/12/08 - prot. 14572-
			Vezzoli Secondo	Nomina del resp. settore del 22/12/08 - prot. 14572-
N° 7 - COMMERCIO E PUBBLICI ESERCIZI - ISTRUZIONE E CULTURA	Brolis Dr. Angelo	Commercio e pubblici esercizi	Delcarro Angelo	Nomina del resp. settore del 22/12/08 - prot. 14573-
		Istruzione	Tadolti Angela	Nomina del resp. settore del 22/12/08 - prot. 14573-
		Biblioteca e Cultura	Morelli Luigi	Nomina del resp. settore del 22/12/08 - prot. 14573-
			Gioia Cristina	Nomina del resp. settore del 22/12/08 - prot. 14573-

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, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
- 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: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (**mansionario privacy**), nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare 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 viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Nella seguente matrice si riassumono i tratti salienti dell'attuale mansionario privacy, come segue:

- sull'asse verticale si riportano i dati oggetto di trattamento, quali emergono dall'analisi effettuata nel paragrafo 1. del presente documento
- sull'asse orizzontale si riportano le unità organizzative ("**strutture di riferimento**") in cui si suddivide l'organizzazione del Titolare
- l'apposizione del simbolo X, in corrispondenza della casella di intersezione tra le due coordinate, significa che una determinata unità organizzativa procede al trattamento dei dati indicati nelle righe:

TIPOLOGIA DEI DATI TRATTATI							
Dati comuni relativi a clienti /cittadini / dipendenti.	X	X	X	X	X	X	X
Dati comuni relativi a fornitori.	X	X	X	X	X	X	X
Dati comuni relativi ad altri soggetti.	X	X	X	X	X	X	X
Dati biometrici relativi al personale e ad altri soggetti.*							
Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti.	X					X	
Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali.				X	X		X
Dati di natura giudiziaria relativi a clienti, fornitori, cittadini, dipendenti e ad altri soggetti.	X	X	X		X	X	X
Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile.	X	X	X	X	X	X	X
Dati di natura sensibile relativi a clienti/fornitori/cittadini.	X	X	X	X	X	X	X
Dati idonei a rivelare lo stato di salute e/o la vita sessuale.	X		X				
Dati idonei a rivelare l'affezione da virus HIV.			X				
* attualmente non trattati							
	1	2	3	4	5	6	7
	UNITA' ORGANIZZATIVE						

La legenda delle unità organizzative ("**strutture di riferimento**") è la seguente:

- 1 – Amministrazione generale
- 2 – Lavori Pubblici
- 3 – Servizi sociali
- 4 – Contabilità e finanza
- 5 – Urbanistica ed Ecologia – Gestione del Territorio e dell'ambiente
- 6 – Polizia Locale e Protezione Civile
- 7 – Istruzione e Cultura / Commercio e Pubblici esercizi

Si allegano:

1. prospetto della struttura organizzativa con i responsabili di settore, i servizi facenti capo agli stessi e il personale assegnato.
2. le banche dati dei trattamenti operati dalle varie strutture e relative finalità.

Sono previsti **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 incaricati dal Titolare, che all'esterno, presso soggetti specializzati.

3. Analisi dei rischi che incombono sui dati

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Nella seguente matrice si procede a una stima del grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

GRADO DI INTERESSE PER I TERZI	ELEVATISSIMO				12 Dati genetici (non trattati)
	ALTO		6 Dati svolgimento di attività economiche		11 Dati idonei a rivelare l'affezione da virus HIV
	MEDIO	1 Dati comuni clienti /cittadini/dipendenti 3 Dati comuni altri soggetti		9 Dati sensibili clienti/fornitori/cittadini	10 Dati stato di salute e/o vita sessuale
	BASSO	2 Dati comuni di fornitori	4 Dati biometrici personale ed altri soggetti. 5 Dati idonei a rilevare la posizione	7 Dati di natura giudiziaria 8 Dati sensibili personale	
	BASSO	MEDIO	ALTO	ELEVATISSIMO	
PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO					

Si nota che un grado di rischio alto, o addirittura elevatissimo, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati
- quelli che costituiscono una importante risorsa, commerciale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita, o trafugamento, dei dati.

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio possono essere suddivise in:

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
 - al verificarsi di eventi distruttivi (incendi, allagamenti, terremoti...)
 - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti)
3. rischio di penetrazione logica nelle reti di comunicazione
4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

1	Bianco = molto basso o assente	Nella seguente tabella si evidenziano i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali. La scala dei simboli da porre nella casella di intersezione varia secondo la legenda in basso. (per esempio bianco corrisponde un'esposizione al rischio modesta; il rosso significa che l'esposizione al rischio è molto elevata.)
2	Verde = basso	
3	Giallo = medio	
4	Arancione = alto	
5	Rosso = molto alto	

TIPO DI RISCHIO	LIVELLO DI RISCHIO														
Rischio d'area, legato al verificarsi di eventi distruttivi	3	3	3	3	3	2	3	3	2	3	3	2	3	3	
Rischio d'area, legato all'accesso non autorizzato nei locali	3	2	1	2	1	3	2	1	3	2	1	3	1	1	
Rischio di guasti tecnici di hardware, software e supporti	1	1	1	3	3	4	3	3	4	3	3	4	2	2	
Rischio di penetrazione logica nelle reti di comunicazione	1	1	1	1	1	1	1	1	1	4	4	4	1	1	
Rischio legato ad atti di sabotaggio e ad errori umani	3	2	2	3	2	2	3	2	2	3	3	3	2	2	
	A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3	E	F	
	TIPI DI STRUMENTI														

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:

- **A1** quelli custoditi in un'area ad accesso non controllato
- **A2** quelli custoditi in un'area ad accesso non controllato in armadi con chiave
- **A3** quelli custoditi in un'area ad accesso controllato

B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:

- **B1** quelli localizzati in un'area ad accesso non controllato
- **B2** quelli localizzati in un'area ad accesso controllato
- **B3** quelli portatili o altri dispositivi mobili

C – Elaboratori in rete privata

- **C1** quelli localizzati in un'area ad accesso non controllato
- **C2** quelli localizzati in un'area ad accesso controllato
- **C3** quelli portatili o altri dispositivi mobili

D – Elaboratori in rete pubblica

- **D1** quelli localizzati in un'area ad accesso non controllato
- **D2** quelli localizzati in un'area ad accesso controllato
- **D3** quelli portatili o altri dispositivi mobili

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti.

F – Altri strumenti (es. basati su dati biometrici).

Nell'elaborare la tabella, si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:

- Il rischio d'area, legato al verificarsi di eventi distruttivi è considerato medio, perché anche se remoto è sempre possibile.
- il rischio d'area, legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato medio e più basso per le aree ad accesso controllato, rispetto a quanto accade per gli altri luoghi in cui si svolge l'attività, con conseguente diminuzione del rischio.

- il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti mobili (Notebook, palmari..etc) che per loro natura e destinazione, sono più soggetti a rotture accidentali di quelli fissi.
- il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro interconnessi e collegati ad una rete di comunicazione accessibile al pubblico (internet) ed considerata alta in caso di connessione ADSL o reti WIRELESS.
- il rischio legato ad atti di sabotaggio o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati è sempre presente ed è maggiore per quelli che sono collegati in rete pubblica o per le zone non ad accesso controllato.

Per facilitare la stesura del capitolo successivo si è redatto la seguente tabella che tenuto conto di quanto detto in precedenza analizza i principali rischi, il loro impatto sui dati e le contromisure necessarie.

FATTORE DI RISCHIO	IMPATTO SUI DATI	CONTROMISURA
Comportamento degli operatori		
- furto di credenziali di autenticazione	Perdita, modifica, furto. Trattamenti non consentiti.	Formazione del personale, procedure di backup e di ripristino dei dati, sistemi di crittografia dei dati.
- carenza di consapevolezza, disattenzione o incuria	Perdita. Trattamenti non consentiti.	Formazione del personale, procedure di backup e di ripristino dei dati
- comportamenti sleali o fraudolenti	Perdita, modifica, furto. Trattamenti non consentiti.	Protezione strumenti e locali, formazione del personale, procedure di backup e di ripristino dei dati, sistemi di crittografia dei dati.
- errore materiale	Perdita. Trattamenti non consentiti.	Formazione del personale, procedure di backup e di ripristino dei dati.
Eventi relativi agli strumenti		
- azione di virus informatici o di codici malefici	Perdita e/o temporanea indisponibilità	Utilizzo di software specializzato sempre aggiornato, procedure di backup e di ripristino dei dati, Formazione del personale.
- malfunzionamento, indisponibilità o degrado degli strumenti	Perdita e/o temporanea indisponibilità	Corretta manutenzione e costante aggiornamento, procedure di backup e di ripristino dei dati
- accessi non autorizzati	Perdita, modifica e furto. Trattamenti non consentiti.	Installato Firewall e implementato sistema di autenticazione, procedure di backup e di ripristino dei dati, Formazione del personale, sistemi di crittografia dei dati.
- intercettazione di informazioni in rete	Modifica e furto. Trattamenti non consentiti.	Installazione Firewall e implementato sistema di autenticazione, sistemi di crittografia dei dati.
- guasto ai sistemi complementari (impianto elettrico etc..)	Perdita e/o temporanea indisponibilità	Installazione di gruppo di continuità e procedure di backup e di ripristino dei dati.
Eventi relativi al contesto		
- accessi non autorizzati a locali / reparti ad accesso ristretto	Perdita, modifica e furto. Trattamenti non consentiti.	Formazione del personale, antifurto e sistemi di protezione locali.
- asportazione e furto di strumenti contenenti dati	Perdita, modifica e furto. Trattamenti non consentiti.	Formazione del personale, antifurto e sistemi di protezione locali .
- eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti a incuria	Perdita.	Formazione del personale, sistemi di protezione locali, procedure di backup e di ripristino dei dati.
- errori umani nella gestione della sicurezza fisica	Perdita e/o temporanea indisponibilità. Trattamenti non consentiti.	Formazione del personale, procedure di backup e di ripristino dei dati.

4. Misure atte a garantire l'integrità e la disponibilità dei dati

Nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal Dlgs 196/2003, e dal disciplinare tecnico in materia di misure minime di sicurezza, allegato a tale decreto sub b).

4.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da :

- sono presenti i dispositivi antincendio come previsto del Dlgs 626/94 e successive modifiche.
- Porte taglia fuoco nell'area Archivio nel semi interrato.

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da :

- Il piano terra e il piano semi interrato della palazzina del Municipio presentano sbarre anti intrusione alla porta principale e a tutte le finestre.
- L'ufficio anagrafe posto al piano terra è protetto da un sistema di allarme.
- L'ufficio Polizia Locale, situato in Via Verdi, 13, al piano terra è protetto da sbarre anti intrusione alla porta principale e a tutte le finestre, inoltre è presente un impianto d'allarme collegato con il 112. Le autovetture e i loro contenuti sono sempre sotto la custodia del personale della Polizia Locale e in alternativa sono custodite all'interno dell'autorimessa protetta da allarme e sistema di videosorveglianza.
- I locali della biblioteca sono protetti da un sistema d'allarme.
- Dopo la chiusura degli uffici, le porte di ingresso di tutti gli uffici vengono chiuse e di fatto diventano aree ad accesso controllato.
- Durante l'orario di apertura esiste una continua vigilanza da parte di personale interno.
- Nelle ore di chiusura esiste un servizio di vigilanza.
- Accesso ristretto alle aree in cui si svolgono i trattamenti più critici, mediante:

- Adozione della regola che i dati più personali (sensibili e giudiziari) sono trattati esclusivamente all'interno dei locali previsti, accessibili ai soli incaricati dei trattamenti ed ai soggetti specificamente autorizzati ad accedervi.

Gli impianti ed i sistemi di cui è dotata l'organizzazione:

- appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno 2010 sono quindi previsti semplicemente interventi di manutenzione e rimpiazzo.

4.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, fotografie, pellicole...), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione.

A tale fine, gli incaricati sono stati dotati di :

- cassettiere con serratura
- armadi chiudibili a chiave
- di speciali archivi chiudibili a chiave
- in alcuni casi di cassaforte

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni delle unità organizzative.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa avviene in luoghi, armadi, casseforti, o dispositivi equipollenti, che possono essere chiusi.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti

- ad alcune persone, aventi la scrivania prospiciente, viene dato l'incarico di vigilare gli archivi, dettando precise istruzioni in merito al fatto che una persona deve essere sempre presente, durante l'orario di apertura dell'archivio, per controllare chi vi accede.
- alcuni dipendenti svolgono la mansione di addetti all'archivio
- le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'incaricato che ha il compito di custodirla

Si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, mediante l'adozione dei seguenti accorgimenti :

- la chiave dell'archivio è affidata, dopo l'orario di chiusura, al titolare o ai responsabili del trattamento, o in alternativa ad uno o più soggetti incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di coloro che hanno richiesto di accedere all'archivio

Gli impianti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari:

- appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per l'anno 2010, sono quindi previsti semplicemente interventi di manutenzione e di sostituzione.

4.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si sono adottate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato
- realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus)
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD...), nei quali siano contenuti dati personali.

Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle **credenziali di autenticazione** per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizzano i seguenti metodi:

- si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
 - immediatamente, non appena viene consegnata loro da chi amministra il sistema
 - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino,)
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che:

- si è impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

Il profilo di autorizzazione non viene in genere studiato per ogni singolo incaricato, ma è generalmente impostato per classi omogenee di incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale). L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, si è dotati di idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus,

Si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

- automatico ogni giorno le nuove impronte virali se disponibili dal sito web del produttore del software antivirus per tutti i pc collegati in rete pubblica.
- ogni settimana le nuove impronte virali installando tramite supporto cd-rom le patches preventivamente scaricate dal sito web del produttore del software antivirus nel caso di strumenti elettronici che non sono in rete .
- Ogni anno alla scadenza di rinnovare l'aggiornamento della versione più aggiornata del software antivirus installato su ogni pc utilizzato all'interno della struttura del Titolare.

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idoneo strumento elettronico, comunemente conosciuto come firewall, che il nuovo codice privacy ha reso obbligatorio per i casi in cui si trattino dati sensibili o giudiziari.

A tale riguardo:

- la nostra organizzazione si è da tempo dotata di tale strumento, per la protezione degli elaboratori in rete collegati alla rete pubblica internet tramite un router con collegamento ADSL . La scelta è caduta su una versione software installata su un pc dedicato dotato di 2 schede di rete che garantisce una protezione perimetrale molto efficace e facilmente aggiornabile .

Si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

- Ogni anno alla scadenza prevista di rinnovare il contratto di aggiornamento del software firewall in modo di ricevere e installare sempre l'ultima versione disponibile considerata la più adatta a fronteggiare le ultime tecniche di intrusione nelle reti informatiche.

Per il trattamento di dati idonei a rivelare lo stato di salute o la vita sessuale, si adottano particolari accorgimenti, con il fine di:

- rendere temporaneamente inintelligibili tali dati, anche a chi è autorizzato ad accedervi: per l'accesso a tali dati, gli incaricati autorizzati devono inserire una ulteriore parola chiave nel documento in mancanza della quale l'accesso ai dati è impedito.

Per garantire ciò è stato installato un sistema di crittografia per i dati più sensibili che riguardano lo stato di salute o la vita sessuale e rivelare l'affezione da virus HIV, in modo che il loro contenuto possa essere letto solo da incaricati in possesso di un particolare codice che permettere la identificazione degli interessati solo in caso di necessità.

Il terzo aspetto riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi.

A tale riguardo:

1. la nostra organizzazione si è da tempo dotata di una metodologia di comportamento per la protezione da malfunzionamenti degli strumenti elettronici, che prevede che una ditta specializzata su richiesta del responsabile di sistema interno del Titolare effettui visite periodiche con cadenza almeno semestrale per verificare tutti gli strumenti in particolare con i quali si trattano dati sensibili o giudiziari ed effettuare la manutenzione preventiva e d'urgenza dell'hardware installato e dell'aggiornamento dei programmi (firewall, sistema operativo, backup) e della loro corretta configurazione.

Per quanto concerne i **supporti rimovibili** (es. floppy disk, dischi ZIP, CD...), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassette chiuse a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Circa le *“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”*, provvedimento emanato dal Garante in data 27/11/2008, si provvederà nell'anno in corso ad applicare idonea procedura per il **controllo dell'attività dell'amministratore di sistema** per assicurare la massima trasparenza sul suo operato.

Infine, secondo quanto indicato dal provvedimento del Garante in data 13/10/2008, particolare attenzione sarà rivolta a contrastare le **minacce potenziali alla riservatezza, integrità e disponibilità dei dati**, in caso di:

- **eventuale reimpiego**, riciclaggio di sistemi informatici e/o apparecchiature elettroniche contenenti dati personali in uso nello svolgimento di attività istituzionali,
- **dismissione** di sistemi informatici e/o di apparecchiature elettroniche dedicate.

Al fine di evitare la messa in circolazione di dati personali che non siano stati cancellati in modo idoneo e di non permettere l'accesso ad essi da parte di terzi non autorizzati, di seguito sono elencate le misure adottate per:

- Reimpiego o riciclo:

Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

Limitatamente ai personal computers con i quali sono trattati dati sensibili, è prevista la cifratura di singoli *file* o gruppi di *file*, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste effettuare la successiva decifrazione.

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

1. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali *wiping program* o *file shredder*) che provvedono, una volta che l'utente abbia eliminato dei *file* da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.

Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni, secondo la velocità del computer utilizzato.

2. Formattazione "a basso livello" dei dispositivi di tipo *hard disk (low-level formatting-LLF)*, laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;

- Smaltimento

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a seconda del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici:

- appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati. Per l'anno 2010, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento, alla manutenzione ed a qualche rimpiazzo.

5. Criteri e modalità di ripristino dei dati

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

Attualmente **esiste un sistema generalizzato** che crea una copia dei documenti cartacei e degli eventuali altri supporti diversi da quelli elettronici. Attualmente il Titolare ha infatti implementato le procedure previste dal cosiddetto “Protocollo informatico” ed ha attivato la funzione di archiviazione ottica dei documenti protocollati.

Per i dati trattati con strumenti elettronici, sono state previste procedure di backup, centralizzate su un server attraverso il quale viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni.

Il salvataggio dei dati trattati avviene come segue:

PROFILI DI BACK_UP – COPIE DI SICUREZZA SU SUPPORTI MAGNETICI

Hardware	Procedura	Supporto	Descrizione	Frequenza	Conservazione
Server 1	demografici – elettorale - contabilità’ – tributi – delibere – protocollo – p.d.o. halley – procedure messi halley – blue’s 2002 – concilia	Nastri a cassetta da 24/40 Gybyte di DDS4	Copie eseguite dal server con procedure automatiche che si attivano ad orario programmato a ciclo settimanale, nelle ore notturne	giornaliera	In cassaforte presso l’immobile ove hanno sede i server. La copia giornaliera è conservata per 15 giorni. La copia del primo giorno lavorativo di ogni mese è conservata per un anno.
Server 1	(1) Dati contenuti nella cartella “Salva” impostata su ogni Personal Computer	Nastri a cassetta da 24/40 Gybyte di DDS4	Copie eseguite dal server con procedure automatiche che si attivano ad orario programmato ogni lunedì a personal computer accesi.	settimanale	In cassaforte presso l’immobile ove hanno sede i server. La copia giornaliera è conservata per una settimana. La copia del primo lunedì di ogni mese è conservata per un anno.
client	Winmark per la gestione delle presenze del personale	Da cartella a cartella su disco fisso di altro client	Eseguito dalla procedura stessa a scadenza mensile previa autorizzazione manuale	mensile	Cartella su hard disk diverso da quello di normale utilizzo, conservata per tutto il mese.

(1) Qualora il titolare della postazione p.c. non provveda a collocare i documenti da salvare nella cartella “Salva” collegata al server, dovrà occuparsi personalmente delle copie di salvataggio con mezzi propri e sarà responsabile dell’eventuale perdita dei dati dovuta a malfunzionamento o rottura della macchina

Periodicamente, con cadenza almeno semestrale vengono effettuate, sotto la responsabilità dell’amministratore di sistema, delle prove di ripristino, mediante l’esecuzione di appositi test di efficacia delle procedure di salvataggio e di ripristino dei dati adottate.

In particolare si precisa che il server 1:

- **dispone di sistemi RAID** (Redundant array of inexpensive disks): si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco, che garantiscono la disponibilità e l’integrità dei dati, anche nel caso di guasto hardware di uno dei dischi che compongono il sistema.
- **dispone di doppio alimentatore**. In modo da garantire la continuità di servizio in caso di guasto di uno degli alimentari.

Essendo su tale pc installati gli applicativi comunali disponibili in rete ai singoli incaricati e i relativi dati e preso atto di quanto prima analizzato si ritiene che l’integrità dei dati e la loro disponibilità siano garantite in caso di guasti allo strumento elettronico in oggetto.

Questo server dispone di gruppo di continuità adeguato per garantire il suo funzionamento in caso di brevi interruzioni di corrente.

I criteri e le modalità di ripristino dei dati, le misure logiche di sicurezza adottate dal Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati.

6. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE, se il terzo destinatario non è italiano.

In ogni caso, il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali
2. di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali
3. di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Qualora il trasferimento dovesse avvenire verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano:

- rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico

- consegnare una copia del documento programmatico sulla sicurezza redatto, ovvero consegnare una copia del certificato di conformità rilasciato da chi ha curato la progettazione e l'attuazione delle misure minime di sicurezza, nel caso in cui il destinatario abbia affidato a soggetti esterni tali compiti.

Allo stato attuale, il quadro sintetico delle attività trasferite a terzi, che comportano il trattamento di dati personali, è il seguente:

FUNZIONE SVOLTA SU DELEGA, CONVENZIONE, ALTRO CHE COMPORTANO TRATTAMENTO DI DATI PERSONALI	SOCIETÀ O COOPERATIVA TITOLARE	RESPONSABILE NOMINATO	SCADENZA INCARICO
Servizio di brokeraggio assicurativo	AON spa di Milano	Bertani Fiorenzo	31/12/2010
Servizio di assistenza domiciliare	Fondazione S. Giuliano di Ciserano	Maffioletti Pierluigi	30/04/2010
Servizio di refezione scolastica e ristorazione collettiva	Punto Ristorazione srl di Gorle	Serravalle Maurizio	31/08/2011
Servizio di accertamento e riscossione dell'imposta comunale sulla pubblicità e dei diritti sulle pubbliche affissioni	AIPA spa di Milano	Snaiderbaur Bruno	31/12/2010
Servizio di trasporto socio-sanitario	Associazione IL SOLE di Verdellino	Cinquarla Elio	31/12/2010
Servizio riscossione TARSU e TIA	EQUITALIA ESATRI S.p.A di Bergamo	Rossi Giancarlo	31/12/2010
Servizio riscossione e rendiconto ICI	EQUITALIA ESATRI S.p.A di Bergamo	Rossi Giancarlo	31/12/2010
Servizio individuazione e recupero evasione fiscale ICI e accesso via internet agli archivi ICI VIOLAZIONI	EQUITALIA ESATRI S.p.A. di Bergamo	Rossi Giancarlo	31/12/2010
Servizio di assistenza tecnica software help desk – uffici diversi - biennio 2010/2011-	IT INNOVAZIONE di Bagnatica	Borchia Stefano	31/12/2011
Servizi educativi presso asilo nido a.s. 2009/2010	Società Cooperativa Sociale CITTA' DEL SOLE Onlus di Bergamo	Ghilardi Ines	31/07/2010
Servizi assistenza scolastica per alunni in situazione di disabilità	Società Cooperativa Sociale CITTA' DEL SOLE Onlus di Bergamo	Ghilardi Ines	31/08/2010
Servizio di manutenzione e assistenza tecnica sistema di gestione ottica dei documenti	MEDIADOC S.r.l. di Peschiera Borromeo	Bailini Paolo	31/12/2010
Trascrizioni cassette audio registrazione sedute consiliari	STENOSERVICE S.n.c. di Forlì	Ortali Daniela	31/12/2010
Consulenza materia IVA	PUBLICONSUL srl di Lovere	Selogni Giuseppina	31/12/2010
Servizio gestione sale centro sociale	AUSER di Verdellino	Piccolo Francesco	31/12/2011
Servizio di manutenzione e assistenza tecnica software demografici - Tributi	EDK EDITORE S.r.l. di Torriana	Pasini Roberto	31/12/2010
Servizio gestione sale per attività del "Centro di incontro"	"ANTEAS" di Bergamo	Dalla Chiesa Giuseppe	28/02/2012

FUNZIONE SVOLTA SU DELEGA, CONVENZIONE, ALTRO CHE COMPORTANO TRATTAMENTO DI DATI PERSONALI	SOCIETÀ O COOPERATIVA TITOLARE	RESPONSABILE NOMINATO	SCADENZA INCARICO
Servizio tesoreria e cassa	BANCA POPOLARE DI SONDRIO	Manzoni Gianluigi e Mondinelli Antonio	31/12/2013
Incarico di completa gestione stipendi anno 2010-2011	ENTI SERVICES snc di Bussolengo	Finezzo Marco	31/12/2011
Utilizzo dei servizi on line	EQUITALIA ESATRI S.p.A. di Milano	Bidasio Ettore	21/07/2012
Servizio gestione istanze relative alla erogazione di: "Bonus tariffa elettrica" – "Bonus tariffa gas"	ASSICISL S.r.l. – CAAF CISL di Bergamo	Nava Fabio	31/12/2010
Servizio gestione istanze relative alla erogazione di: "Bonus tariffa elettrica" – "Bonus tariffa gas"	CAF ACLI s.r.l. – Acli Service Bergamo s.r.l. di Bergamo	Farina Michele	31/12/2010
Servizio gestione istanze relative alla erogazione di: "Bonus tariffa elettrica" – "Bonus tariffa gas"	UILSER S.r.l. – CAF di Bergamo	Catia Ravasio	31/12/2010
Servizio gestione istanze relative alla erogazione di: "Bonus tariffa elettrica" – "Bonus tariffa gas"	C.S.F. CGIL Bergamo S.r.l. – CGIL CAAF di Bergamo	Viero Francesco	31/12/2010
Visione telecamere installate nel territorio comunale	STAZIONE CARABINIERI DI ZINGONIA	Tucci Gerardo (Luogotenente)	=====

7. 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.

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.

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.

8. Dichiarazioni d'impegno e firma

Il presente documento, redatto nel marzo 2010 viene firmato in calce da:

- Bacis Giovanni, in qualità di rappresentante legale del Titolare
- Martinelli Gianfranco, in qualità di responsabile per la sicurezza.

Il presente Documento programmatico sulla sicurezza è stato sottoposto per l'approvazione della Giunta Comunale e successivamente trascritto nel libro che riporta le delibere prese dallo stesso.

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

Una sua copia verrà consegnata:

- a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali .

Nella relazione accompagnatoria del bilancio di esercizio si riferisce dell'avvenuta redazione del presente documento, che costituisce:

- aggiornamento per l'anno 2010 del Documento programmatico sulla sicurezza

Luogo e data.....

Firma del rappresentante legale del Titolare.....

Firma del responsabile per la sicurezza.....