COMUNE DI MELLE (CN)
ALLEGATO DGC N. 012 DEL 16/03/201

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi del D.Lgs. 196/2003

con riferimento alle Misure di Sicurezza di cui dagli artt. dal 31 al 36

ed al Disciplinare Tecnico di cui all'Allegato B al Codice

INDICE

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ai sensi del D.Lgs. 196/2003

Ai sensi degli artt. dal 31 al 36 del Decreto Legislativo 196 del 30 giugno 2003 (d'ora in avanti indicato come "Testo Unico"), ed in relazione a quanto previsto dall'Allegato B al predetto decreto, il Comune di Melle adotta il seguente Documento Programmatico sulla Sicurezza (d'ora in avanti indicato più sinteticamente come "DPS").

1. PREMESSE

Premesso che:

- Il Comune di Melle effettua, ai sensi del Testo Unico sulla Privacy, trattamenti di dati personali;
- Il Comune di Melle, ai sensi della medesima norma è da considerare "titolare" del trattamento dei dati personali;
- Il trattamento dei dati è effettuato tanto attraverso l'utilizzo di documenti cartacei, quanto con il ricorso ad elaboratori elettronici;
- Il trattamento dei dati interessa sia dati genericamente "personali", sia dati personali "sensibili", così come definiti rispettivamente dall'art. 4, comma 1, lett. b) e d) del Testo Unico;
- Il Comune di Melle aveva in passato approvato l'adozione delle Misure Minime di Sicurezza previste dal DPR 318/99 che con il presente Documento vengono aggiornate.

Si stabilisce che:

Il trattamento dei dati personali, specialmente per quanto concerne l'adozione delle misure minime di sicurezza - così come regolamentate dall'art. 31 e dall'Allegato B del Testo Unico – e di altre eventuali misure di sicurezza, sia svolto in conformità alle indicazioni contenute nel DPS, il quale è stato steso al fine di:

- conferire dignità documentale al processo di adeguamento alla normativa sulla riservatezza dei dati personali, svolto nei termini previsti dalla stessa;
- descrivere lo stato delle cose alla data odierna, cui si riferisce la presente verbalizzazione, con la precisazione che il documento rappresenta un'attestazione di quanto esisteva già in passato e di cui ora si prende formalmente atto.

2. ANALISI DEI RISCHI

La valutazione dei rischi cui sono esposti i dati trattati dal Comune di Melle è stata effettuata tenendo presente che:

- tutti i locali del Comune di Melle sono situati presso un unico sito, avente sede nell'edificio di Piazza G. Marconi, 1. Altri locali rilevanti ai fini del trattamento dei dati e quindi della disciplina sulla privacy sono la Biblioteca Comunale situata in Via Carrera, n.3.
- la palazzina è divisa in tre piani, di cui uno è il piano terreno. Al piano terreno è situata l'entrata libera a tutti e il garage; al primo piano sono ubicati gli uffici tecnico, ragioneria, tributi, segreteria, protocollo, commercio e anagrafe/stato civile ed elettorale. Al secondo piano è situata la sala del consiglio. Nella maggior parte di questi locali sono effettuati trattamenti rilevanti ai fini dell'applicazione del presente DPS, anche di dati sensibili, per cui i luoghi di lavoro devono sottostare alle più restrittive e rigorose norme sulla protezione di simili dati.

Al piano terra e al primo piano viene conservato l'archivio cartaceo in locali chiusi a chiave;

- in tutti i locali menzionati sono conservati e trattati informazioni personali in forma cartacea ed attraverso l'utilizzo di strumenti elettronici. I terminali collegati in rete tra di loro sono tre. Presso la Biblioteca comunale sono situati un PC non collegati in rete;
- l'edificio non è provvisto di un impianto di allarme relativo ad evitare intrusioni di soggetti dall'esterno, e non esistono contratti di assistenza con istituti di vigilanza privata. L'edificio della Biblioteca non è provvisto di un impianto di allarme relativo ad evitare intrusioni di soggetti dall'esterno, e non esistono contratti di assistenza con

istituti di vigilanza privata

Per quanto riguarda la struttura fisica di ogni Ufficio, possiamo sintetizzare che:

ogni locale è dotato di una o più porte d'accesso munite di serratura, nonché di finestre con maniglie,

porte e finestre sono in buono stato di manutenzione e conservazione,

ogni Ufficio ha a disposizione armadi e cassetti dotati di serratura.

In considerazione di tali elementi, si è pervenuti alla conclusione che:

- i dati trattati dal Comune di Melle sono esposti agli ordinari rischi propri di qualsiasi sito fisicamente accessibile, oltretutto attenuati dalla congruità della dotazione strutturale e dall'assenza, in passato, di significative infrazioni negli edifici ove vengono effettuati i trattamenti;
- dipendenti, collaboratori ed ogni altro soggetto Incaricato, non costituiscono, con il proprio comportamento che si deve conformare alle prescrizioni ed indicazioni ricevute, un rilevante fattore di rischio per i dati trattati, ma – poiché le mansioni risultano particolarmente flessibili e vaste – essi devono essere adeguatamente responsabilizzati e controllati;
- le postazioni di lavoro meccanizzate non costituiscono un particolare fattore di criticità, poiché beneficiano – in termini di sicurezza fisica – dell'adeguatezza della struttura complessiva e – in termini di sicurezza logica – sono gestite da soggetti che devono seguire precise indicazioni e prescrizioni volte a ridurre al minimo ogni possibile danno proveniente dall'esterno (virus, sabotaggi, ecc. anche proveniente dal collegamento ad Internet).

Riportiamo una Tabella di Analisi e di riassunto dei principali rischi, dal punto di vista dell'applicazione della normativa sulla Privacy, a cui la Ns. struttura potrebbe potenzialmente andare incontro.

Analisi dei rischi

Rischi		Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamenti degli operatori	sottrazione di credenziali di autenticazione	Alta
	carenza di consapevolezza, disattenzione o incuria	Media
	comportamenti sleali o fraudolenti	Alta
	errore materiale	Da Bassa ad Alta in relazione all'ambito delle conseguenze dell'errore
	altro evento	Media (in relazione al tipo di Evento)
Eventi relativi agli strumenti	azione di *virus* informatici o di programmi suscettibili di recare danno	Alta per la maggior parte dei trattamenti Bassa ove esista documentazione cartacea di riferimento
	spamming o tecniche di sabotaggio	Alta
	malfunzionamento, indisponibilità o degrado degli strumenti	Alta
	accessi esterni non autorizzati	Alta
	intercettazione di informazioni in rete	Media
	altro evento	Media (in relazione al tipo di Evento)
Eventi relativi al contesto	accessi non autorizzati a locali ad accesso ristretto	Media
	sottrazione di strumenti contenenti dati	Bassa (in relazione all'esistenza di tutele all'accesso ai dati sugli strumenti)
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.) nonché dolosi, accidentali o dovuti ad incuria	Alta
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Media
	errori umani nella gestione della sicurezza fisica	Media
	altro evento	Media (in relazione al tipo di Evento)

3. ELENCO DEI TRATTAMENTI

I trattamenti dei dati personali posti in essere dal Comune di Melle, in relazione a quanto definito dal Testo Unico, sono svolti in relazione alle finalità tipiche di un Ente Pubblico, con particolare riferimento ai compiti che la legge attribuisce agli Enti Locali. I trattamenti dei dati vengono svolti attraverso l'utilizzo di diverse banche dati, sia cartacee che informatiche. Allo stato attuale i trattamenti effettuati dalla struttura, possono essere classificati con il seguente schema, che introduce sia una divisione relativa alla natura dei dati trattati (C-comuni, S-sensibili), sia in relazione agli strumenti di trattamento utilizzati (C-carta, I-informatici). In quest'ultimo caso verrà segnalata la prevalenza del trattamento, considerando quindi quali siano le Banche Dati prevalentemente utilizzate a tal fine (cioè se sono prevalenti i dati provenienti da strumenti informatici o viceversa da documenti cartacei).

Tabella 1.1: Elenco dei trattamenti

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati (Banca dati prevalente)
1.r	Delibere e determine	C	S	Ragioneria	NO	C
2.r	Protocollo	C	S	Ragioneria	NO	I
3.r	Contabilità	C		Ragioneria	NO	I
4.r	Tributi	C	S	Ragioneria	NO	I
5.r	Personale	C	S	Ragioneria	ALMA SPA	I
6.r	Commercio	C		Ragioneria		C
7.r	Anagrafe/stato civile/elettorale	C	S	Servizi Demografici	NO	I
8.t	Concessioni edilizie	C	S	Ufficio Tecnico	NO	C
9.r	Multe	C		Ragioneria	NO	C
10.r	Assistenza/cultura/scuola	C	S	Ragioniera	NO	C

Le strutture all'interno dell'organizzazione complessiva del Comune di Melle che si occupano del trattamento di dati personali, anche in relazione ai compiti loro assegnati sono le seguenti:

Tabella 2.1: Strutture preposte ai trattamenti

Struttura	Interna/ Esterna	Eventuale Responsabile	Trattamento operati dalla struttura	Compiti della struttura
Ragioneria	I		1.r, 2.r, 3.r, 4.r, 5.r, 6.r, 7.r, 9.r, 10.r	Adempimenti relativi ai dipendenti, amministrativi, contabili, fiscali e tributari Gestione ed aggiornamento dati anagrafici Multe e sanzioni ed archiviazione atti Assistenza servizi alle persone
Ufficio Tecnico	I		8.t	Gestione pratiche edilizie ed opere pubbliche

4. DISTRIBUZIONE DEI COMPITI

In base alla valutazione dei rischi ed all'esame della tipologia, dell'entità e della distribuzione delle attività condotte dal Comune di Melle nell'attuazione dell'attività lavorativa della propria organizzazione:

- ciascun dipendente e collaboratore è stato esplicitamente incaricato ed autorizzato, mediante apposito provvedimento di Incarico, al trattamento dei diversi tipi di dati;
- gli incarichi – così come la responsabilità per la conservazione dei dati - vengono conferiti personalmente al momento dell'inserimento di una nuova figura all'interno della struttura dell'ente;
- ciascun Incaricato può operare, per il trattamento dei dati, esclusivamente all'interno delle mansioni assegnate e in riferimento alle informazioni ed alle Banche dati disponibili relative alla propria categoria di appartenenza;
- i soggetti che trattano dati riferiti all'attività del Comune, ma che, per qualifica attribuita, od in relazione alla concreta attività svolta, non rivestono la figura di Incaricati, sono stati opportunamente autorizzati al trattamento, mediante specifica

Convenzione che riguarda l'utilizzo dei dati e le diverse responsabilità di ognuno, come esaminato nel seguito del presente paragrafo.

L'attuale organizzazione interna della struttura, sempre in relazione ai soggetti coinvolti nel trattamento di dati rilevanti ai fini del Testo Unico, è la seguente:

- *Consiglio Comunale e Giunta;* tali organi non hanno poteri diretti di gestione delle banche dati, né operano eseguendo trattamenti. Tuttavia, al fine di svolgere appieno il mandato loro conferito, ogni consigliere ha poteri di consultazione di ogni documento, sia cartaceo che informatico, anche contenente dati sensibili;
- *Altri Uffici così come segnalati nella precedente Tabella 2.1.*

Gli altri dipendenti dell'Ente non svolgono attività rilevanti ai fini del Testo Unico.

In relazione a quanto è necessario stabilire con il presente DPS, vanno segnalati diversi soggetti che, pur non essendo alle dipendenze della struttura, anche in considerazione di quanto segnalato alla Tabella 1.1 di questo documento, partecipano attivamente al trattamento di dati rilevanti ai fini del Testo Unico sulla Privacy. Tali soggetti agiscono in base a specifici incarichi od appalti; la seguente tabella documenta l'attuale situazione del Comune in relazione ai soggetti esterni alla struttura.

Tabella 3.1: Strutture esterne preposte ai trattamenti (anche eventuali)

Struttura	Attività	Trattamenti in cui interviene il soggetto	Motivo dell'intervento
ALMA SRL	Elaborazione Paghe	5.r	Incarico
LA MANETO di Dovo Silvie di Sampeyre	Lavori di Pulizia		Incarico
BALSAMO PAOLO	Assistenza/manutenzione informatica hardware e rete informatica		Incarico
SINTECOP	Assistenza Software		Appalto
TECNICAL DESIGNE	Assistenza Programma (pratiche edilizie)		Incarico
EQUITALIA	Riscossione tributi		Incarico

In dettaglio, il coinvolgimento dei predetti soggetti esterni, è il seguente:

- *Società e ditte che effettuano la manutenzione dei Personal computers, dei softwares e delle reti informatiche e/o elaborazione dati*. Tali soggetti operano in base a specifica autorizzazione, recante nel dettaglio compiti e i limiti nell'espletamento dell'attività di assistenza. In particolare, queste Ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione, o semplicemente è necessario verificare il funzionamento di un programma o di una attrezzatura informatica. A tal fine è praticamente obbligatorio accedere alle base di dati presenti sui personal computers o all'interno dei programmi software, evidenziando così una conoscenza di dati personali che di per sé, non è collegata allo scopo per cui la Ditta effettua la propria attività. Ai sensi del punto 25 del Disciplinare Tecnico allegato al D.Lgs. 196/2003, se l'adozione delle misure minime di sicurezza viene affidata a soggetti esterni alla propria struttura, quali i fornitori di programmi software dedicati, il Titolare del trattamento riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare Tecnico richiamato.

  Pertanto l'autorizzazione/accordo concluso con ognuno dei suddetti soggetti indicherà i limiti e le responsabilità a cui la Ditta andrà incontro nel caso in cui i dati accidentalmente conosciuti vengano comunicati o diffusi in violazione della normativa sulla Privacy. Si precisa che naturalmente non sarà posta in essere alcuna violazione di legge qualora all'interno della prestazione offerta da queste Ditte siano comprese anche determinate attività di elaborazione dati. In particolare l'attività di elaborazione paghe comporta il trattamento dei dati da parte della ditta ALMA SRL che ha ricevuto la nomina di Responsabile in cui è dettagliatamente individuato l'ambito della prestazione e le responsabilità conseguenti che le parti si assumono;

- *Società e ditte che svolgono attività di pulizia dei locali*. Tali soggetti possono essere variamente organizzati, ed operano su specifico incarico del Comune. Valgono le medesime precisazioni sulla circostanziata indicazione delle responsabilità e del controllo sulle prestazioni ricevute di cui al punto precedente. La Ditta incaricata delle pulizie dei locali può operare sotto il controllo di dipendenti dell'Ente, od in locali in cui il/i lavoratore/i è/sono temporaneamente solo/i, e ciò potrà avvenire in qualsiasi ambiente. L'Autorizzazione conferita tiene specificatamente conto di questa modalità

organizzativa, sottolineando l'ambito e la disciplina delle responsabilità a cui si va incontro.

Tutti i soggetti sinora elencati, in relazione a quanto specificato per ognuno di essi, sottoscrivono un accordo con il Comune che disciplina esattamente gli ambiti di responsabilità e di obblighi che le parti sono tenute ad assumere e che si impegnano ad effettuare. Tutte le Ditte ed i soggetti che operano attraverso propri dipendenti e collaboratori si obbligano a rendere edotti queste persone di tutto quanto previsto dagli accordi ed in generale dalla normativa sulla privacy.

L'affidamento all'esterno (outsourcing) di parti di attività di trattamento dati relativi al Comune di Melle comporterà l'obbligo, identificato specificatamente all'interno del contratto di servizio o di elaborazione, da parte del terzo di applicazione dell'intera normativa sulla privacy, sia, a puro titolo esemplificativo in relazione alle modalità di trattamento e comunicazione dei dati, sia soprattutto in relazione alle Misure di Sicurezza.

5. DISPOSIZIONI SULL'ACCESSO AI LOCALI ED AI DATI PERSONALI

Poiché il rischio da eliminare riguarda il potenziale trattamento o la conoscenza di dati personali da parte di soggetti non autorizzati, evidenziamo le disposizioni sull'accesso ai locali del Comune di Melle da parte di altri soggetti (utenti, tecnici e manutentori, ecc.), che riguardano le misure di sicurezza minime che la struttura attualmente applica.

A) MISURE DI SICUREZZA FISICHE

Richiamando, per una parte delle informazioni necessarie, le indicazioni fornite all'inizio del presente Documento sulla sicurezza, dettagliamo altre Misure specifiche relative ai locali ed agli Uffici in cui la conservazione ed il trattamento dei dati personali assumono una importanza rilevante.

Accesso ai locali

Gli accessi alle parti comuni dell'edificio devono essere chiusi (a chiave nel caso delle porte) negli orari in cui il Comune è chiuso al pubblico. Negli orari di apertura al pubblico, nessun dato personale deve essere posto in vista, o deve essere facilmente accessibile o riconoscibile a chiunque.

Si richiamano inoltre le disposizioni già segnalate nel secondo paragrafo relativo

all'Analisi dei Rischi. Vediamo ora le disposizioni riguardanti specifici locali:

- ***Uffici***

L'accesso agli Uffici amministrativi è strettamente controllato da parte degli Incaricati che effettuano trattamenti di dati personali. Durante il normale orario di apertura degli Uffici, l'accesso ai dati è controllato dai rispettivi incaricati e qualora, per motivi diversi, un Ufficio rimanga temporaneamente vuoto, l'incaricato è obbligato a chiudere a chiave la porta d'accesso dello stesso e custodire la copia di chiavi che ne permettono l'apertura (ovvero consegnarla al collega o ad altro soggetto che comunque abbia diritto ad espletare la propria attività nel medesimo Ufficio).

In ogni caso, ciascun incaricato deve rendere i dati personali specificamente trattati non consultabili o visibili da parte di eventuali terzi che abbiano diritto ad accedere all'Ufficio né al collega che stia svolgendo il proprio lavoro nel medesimo locale. I terzi che possono accedere agli Uffici negli orari di apertura e/o di chiusura sono espressamente determinati in apposite autorizzazioni loro conferite, nelle quali sono indicate le responsabilità loro riferite, quale ad esempio il personale di pulizia, come già evidenziato nel precedente paragrafo.

Tutti gli incaricati devono provvedere a non lasciare mai, in loro assenza, porte e finestre dei rispettivi Uffici aperte. Gli accessi specifici (cassetti, armadi, ecc.) vanno chiusi a chiave sempre, le porte solo in assenza degli addetti dai rispettivi Uffici. Tutti i dati sensibili contenuti su documenti cartacei devono sempre essere conservati dentro armadi o contenitori chiusi a chiave.

- ***Locali archivio***

Gli archivi storici e correnti degli atti comunali sono situati sia al piano terreno che al primo piano; tali locali devono essere chiusi a chiave ed i dati conservati devono essere riposti in modo organizzato e sistematico, salvo che non rivestano più alcuna utilità per l'attività ordinaria di trattamento.

Istruzione per Trattamenti dati cartacei:

In relazione alle Misure di Sicurezza Fisiche, si ritiene fondamentale evidenziare le istruzioni al trattamento riguardanti la complessiva attività del Comune, la cui applicazione pratica risulta essere di vitale importanza per la concreta applicazione del

presente Documento. In particolare tutte le informazioni riportate su documenti cartacei, delle quali si abbia effettiva esigenza di consultazione, devono essere prelevate e detenute in base alla loro attinenza e pertinenza con il trattamento richiesto.

Gli archivi sono ad accesso selezionato, cioè è possibile ricercare ed estrarre esclusivamente i dati necessari per il trattamento. Se si tratta di dati sensibili o giudiziari, ai sensi dell'art. 4, comma 1, lettere d) ed e) del Testo Unico, gli incaricati devono utilizzare esclusivamente i dati strettamente necessari allo svolgimento delle proprie mansioni ed immediatamente restituirli al termine delle operazioni.

I dati sensibili e giudiziari, così come sopra definiti, devono essere conservati dentro contenitori muniti di serratura. Se una o più informazioni devono rimanere a disposizione per un trattamento prolungato o continuo, l'incaricato deve essere sempre presente nel locale ove avviene il trattamento ed essere in grado di impedire a terzi di vedere la documentazione in uso. Nel caso in cui sia indispensabile l'accesso al locale da parte di terzi, l'incaricato provvede preventivamente a riporre tutti i dati personali in consultazione nei relativi siti protetti.

Tutti i soggetti, interni o esterni all'ente, che possono accedere all'edificio o anche ai dati cartacei sono muniti di esplicita autorizzazione, recante in dettaglio le regole per il corretto trattamento dei dati e/o i limiti e le responsabilità connesse al loro diritto di accesso. Tali autorizzazioni sono periodicamente controllate, al fine di verificare la loro osservanza ed adeguatezza alle condizioni di espletamento dei servizi ed in relazione alle motivazioni per le quali sono state assegnate.

B) MISURE DI SICUREZZA INFORMATICHE

Si riportano le principali misure di sicurezza da utilizzare nel trattamento informatico dei dati, che devono essere seguiti da tutti i soggetti coinvolti nell'attività del Comune. Tali comportamenti riguardano sia l'ambito strutturale minimo che i sistemi informatici devono possedere, sia l'ambito delle istruzioni che sono state fornite ai diversi incaricati di ogni settore.

Attualmente gli strumenti informatici utilizzati sono tre Personal computers tutti collegati in rete situati presso gli Uffici Amministrativi, oltre ad un PC utilizzato dagli addetti della Biblioteca Comunale.

Le indicazioni che vengono evidenziate con il presente documento riguardano l'attuale dotazione informatica dell'Ente, ma dovranno essere comunque prese a riferimento anche in relazione a variazioni che ne modifichino la configurazione, come ad esempio la creazione di altre reti, o l'aggiunta di nuovi Personal Computers stand alone.

Istruzione per Trattamenti dati informatici

Le parole chiave di qualunque tipo devono rispettare le seguenti regole generali. Esse:

- devono essere composte da almeno 8 caratteri alfanumerici;
- non devono essere nomi di persona, né date di nascita;
- gli incaricati devono adottare le dovute cautele per assicurare la segretezza di ogni password assegnata. Devono altresì garantirne l'aggiornamento tempestivo e la disponibilità, se la password viene utilizzata da più soggetti, oppure se deve essere conservata al fine di rendere possibile un intervento in caso di prolungata assenza o impedimento che renda indispensabile e indifferibile intervenire sul sistema per esclusive necessità di operatività e di sicurezza;

Altre regole più specifiche verranno segnalate in relazione a determinati ambiti di utilizzo delle parole chiave.

A tutela delle informazioni contenute su supporti informatici e derivanti da trattamenti compiuti per mezzo di elaboratori sia in rete che non, si dispone la predisposizione, per ciascun personal computer in uso, di una parola chiave all'accensione dello stesso (password di BIOS), conosciuta dagli utenti della specifica postazione di lavoro. Sono tali i soggetti che operano all'interno del medesimo locale, o che per esigenze di consultazione dei dati, hanno necessità che un determinato personal sia acceso per poter esaminare una serie di informazioni essenziali per uno specifico trattamento.

Su ogni computer, in rete o meno, deve inoltre essere attivata la funzione di oscuramento o copertura con decorazioni di quanto visualizzato sul monitor, in assenza dell'operatore (screen saver): essa deve essere impostata in modo da entrare in azione in assenza di input per un periodo al massimo pari a 5 minuti e richiedere una parola chiave per essere disattivata. Tale parola chiave, soprattutto nel caso di elaboratori non in rete ad uso promiscuo, deve essere nota a tutti gli utenti della postazione, così come prima definiti.

Sia la password di BIOS che la password di screen saver devono unicamente seguire le regole minime di determinazione delle parole chiave, di cui in precedenza.

Tutti gli elaboratori devono essere protetti da programmi anti-virus contro il rischio di intrusione ad opera di virus informatici, che potrebbero essere introdotti inavvertitamente anche dal personale interno, mediante inserimento di supporti di memoria (floppy disk, cd-rom ed altro). La costante attività di tali programmi deve essere verificata almeno semestralmente e almeno in tali occasioni si procede all'aggiornamento degli stessi.

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 (anti-virus). Nel caso di trattamento informatico di dati sensibili o giudiziari deve essere attivata la protezione contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici (firewall).

In relazione alle modalità di trattamento dei dati, tutte le informazioni che vengono temporaneamente salvate su supporti rimovibili (es. floppy disk) sono trattate sotto la totale responsabilità degli incaricati, i quali dovranno provvedere alla loro conservazione dentro contenitori chiusi a chiave, provvedendo eventualmente a dei doppi salvataggi per evitare la perdita dei dati.

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. Allo stesso modo gli incaricati non possono portare al di fuori dell'edificio tali supporti e, qualora questi ultimi contengano dati sensibili, sono tenuti a formattarli, purché i dati stessi siano stati registrati – se necessario - nella memoria fissa degli elaboratori e non si debba disporre di una copia su supporto rimovibile, che va comunque conservata nei cassetti ed armadi chiusi a chiave, analogamente ai dati cartacei. Ogni utilizzo o trasporto all'esterno di questi supporti è solamente ammesso per esigenze di semplificazione e di immediatezza dei trattamenti, ma è effettuato sotto la piena e totale responsabilità degli Incaricati.

Per l'utilizzo dei programmi dedicati e della rete informatica è assegnata inoltre ad ogni

utente una o più credenziali di autenticazione che, oltre a seguire le regole delle parole chiave di cui sopra, devono avere le seguenti caratteristiche e devono essere utilizzate nel seguente modo:

- la credenziale è una sola nel caso in cui il soggetto incaricato viene unicamente identificato al momento del suo ingresso nella rete, con una sua configurazione che gli permette l'accesso ai propri programmi e documenti relativi alle mansioni assegnate;
- la credenziale è più di una nel caso in cui il soggetto va identificato nel momento di accesso a più programmi specifici che necessitano singolarmente di una password. Se il programma è uno solo, o i programmi da utilizzare e consultare possono ricomprendere una configurazione unica, la credenziale rimane unica;
- la/e credenziale/i di autenticazione devono essere di almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, di un numero di caratteri pari al massimo consentito e non deve essere banale né facilmente riconducibile al soggetto a cui è/sono assegnata/e;
- l'incaricato è tenuto a modificare la/e credenziale/i di autenticazione al primo utilizzo e successivamente almeno una volta ogni trimestre;
- dovute cautele devono essere adottate per assicurare la segretezza della componente riservata della/e credenziale/i assegnata;
- è garantita la massima segretezza – secondo le modalità operative concordate col titolare/responsabile – nell'accesso ai dati o strumenti elettronici da parte di terzi in caso di prolungata assenza o impedimento che renda indispensabile e indifferibile intervenire sul sistema per esclusive necessità di operatività e di sicurezza;
- la medesima credenziale di autenticazione, per quanto riguarda il codice per l'identificazione, non può essere assegnata ad altri incaricati, neppure in tempi diversi;
- le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Il codice per l'identificazione deve essere composto da caratteri alfanumerici, ma può contenere alcuni o tutti gli elementi del nome e cognome del destinatario.

Ulteriori istruzioni riguardano il salvataggio dei dati che deve essere effettuato con frequenza almeno settimanale. Il salvataggio può avvenire indistintamente attraverso un salvataggio su CD in maniera da garantire al meglio la disponibilità dei dati nel caso in cui sopraggiungessero problemi relativi all'utilizzo degli strumenti informatici o della rete che impedisca il trattamento dei dati. In caso di danneggiamento dei dati o degli strumenti elettronici in modo definitivo, le procedure di ripristino danno la garanzia di ripristinare l'accesso ai dati in tempi non superiori a sette giorni.

6. PREVISIONE DI INTERVENTI FORMATIVI

Gli incaricati del trattamento, ai sensi del punto 19.6 del Disciplinare Tecnico allegato al Testo Unico, devono essere adeguatamente formati al fine di essere resi 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 e delle responsabilità che ne derivano.

Gli interventi formativi dovranno essere posti in essere nei confronti di ogni incaricato almeno annualmente, secondo modalità e metodologie che verranno stabilite in relazione alle mansioni ed alle caratteristiche specifiche del soggetto coinvolto nella formazione. Di preferenza una corretta formazione verrà effettuata attraverso la frequentazione di corsi ad hoc, organizzati da soggetti dotati di esperienza e conoscenza della materia. In relazione al fatto che trattasi di un nuovo ed ulteriore adempimento, nel caso di oggettiva impossibilità a partecipare a dei corsi, anche in relazione all'assenza di disponibilità sul mercato di soggetti formatori, verrà data preferenza nella partecipazione ai soggetti dotati di maggiore responsabilità nel trattamento dei dati ed in generale nella gestione dell'intero Ente.

In sede di prima applicazione della misura, ogni incaricato dovrà comunque documentare di aver adempiuto all'obbligo formativo, nell'arco di un anno e mezzo successivi all'approvazione del presente DPS. Successivamente l'obbligo di formazione sarà annuale. I nuovi assunti, le cui mansioni saranno rilevanti ai fini del trattamento dei dati personali, dovranno adempiere all'obbligo almeno entro i dodici mesi

dall'entrata in servizio.

Nel caso di introduzione di nuovi significativi strumenti legislativi o di qualunque genere che rivestano comunque un rilevante rispetto alla materia del trattamento di dati personali, la formazione dovrà essere garantita agli interessati nel tempo massimo di sei mesi dall'evento.

CONCLUSIONI ED ISTRUZIONI PER L'AGGIORNAMENTO DEL DPS

Le misure di sicurezza descritte, anche in relazione all'attuale organizzazione informatica del Comune, risultano interamente applicate alla data di redazione del presente documento, ad eccezione dell'esistenza di un firewall adeguato, che è finalizzato ad impedire l'accesso ai dati conservati sui personal da parte di hackers od altri soggetti che volessero utilizzare i collegamenti Internet per penetrare all'interno del sistema.

Il presente DPS sarà aggiornato ai sensi di legge entro il 31 marzo di ogni anno, o diversa scadenza che verrà eventualmente stabilita da norme o da disposizioni future. Qualora intervengano fatti rilevanti relativi all'organizzazione del Comune, od altri fatti comunque ritenuti importanti, il documento verrà aggiornato senza indugio. In tutti i casi l'aggiornamento potrà essere effettuato anche soltanto per mezzo di richiamo ad integrazione della presente scrittura.

Luogo e data

MELLE, li 16 MAR. 2012

Il Sindaco
IL SINDACO
FINA Giovanni

COMUNE DI MELLE
Prov. di CUNEO