



COMUNE DI OSNAGO

PROVINCIA DI LECCO

Viale Rimembranze, 3 - Tel. 039952991 - Fax 0399529926
Codice Fiscale 00556800134

DELIBERAZIONE N° 62 DEL 29/03/2011

Trasmessa in elenco ai Capigruppo con nota Prot. n. 7186

ORIGINALE

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: DECRETO LEGISLATIVO 196/03 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" - ALLEGATO B: AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA PER L'ANNO 2011

L'anno duemilaundici, addì ventinove del mese di marzo alle ore 18.30, nella Sala delle Adunanze.

Previa l'osservanza di tutte le formalità prescritte dalla vigente Legge, vennero oggi convocati a seduta i componenti la Giunta Comunale.

All'appello risultano:

| | |
|--------------------|-----------|
| STRINA DOTT. PAOLO | Sindaco |
| CAGLIO GABRIELE | Assessore |
| BELLANO PIERALDO | Assessore |
| LORENZET DANIELE | Assessore |
| POZZI ALESSANDRO | Assessore |
| TIENGO ANGELO | Assessore |

| Firma Presenze |
|----------------|
| SI |
| NO |
| SI |
| SI |
| SI |
| NO |

PRESENTI: 4

ASSENTI: 2

Assiste all'adunanza IL SEGRETARIO GENERALE RENDA DOTT.SSA ROSA la quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti il Sindaco, Sig. DOTT. PAOLO STRINA, assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.



COMUNE DI OSNAGO

PROVINCIA DI LECCO

Viale Rimembranze, 3 - Tel. 039952991 - Fax 0399529926
Codice Fiscale 00556800134

OGGETTO: DECRETO LEGISLATIVO 196/03 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" - ALLEGATO B: AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA PER L'ANNO 2011.

LA GIUNTA COMUNALE

Richiamata la propria deliberazione n. 101 del 2.7.2004 con la quale è stato approvato (e poi aggiornato con deliberazioni G.C. n. 98 del 24.6.2005, n. 44 del 31.3.2006, n. 46 del 30.3.2008, n. 50 del 27.3.2009 e n. 57 del 6.4.2010), ai sensi del punto 19 dell'allegato B al *D.Lgs. 196/03 "codice in materia di protezione dei dati personali"*, apposito "DOCUMENTO PROGRAMMATICO SULLA SICUREZZA", nel quale sono stati indicati:

1. l'elenco dei trattamenti di dati personali dell'ente;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
6. la previsione di interventi formativi degli incaricati del trattamento;
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
8. per i dati cosiddetti "sensibili", l'individuazione dei criteri specifici di sicurezza;

Dato atto che il termine per l'aggiornamento del DPS (per gli enti che hanno già provveduto alla sua adozione) è previsto entro il 31 marzo 2011;

Rilevato che comunque l'efficacia delle misure di sicurezza deve essere oggetto di controlli periodici da eseguirsi con cadenza almeno annuale, ragioni per cui il documento programmatico della sicurezza deve essere ora aggiornato tenendo conto delle intervenute variazioni alla struttura organizzativa ed alla gestione operativa dei trattamenti nel corso del 2010;

Preso atto che la redazione, e conseguentemente i relativi aggiornamenti, del documento programmatico sono posti a carico del Titolare "anche attraverso il responsabile, se designato";

1. Richiamato il decreto sindacale prot. n. 16108 in data 15.12.2009 con il quale il Titolare ha designato Amministratore di Sistema, come definito dal Provvedimento del 27.11.2009 del Garante per la Protezione dei dati personali, il Sig. Crippa Gianfranco, quale rappresentante legale della ditta GFC, nella sua qualità di incaricato per l'assistenza tecnica e consulenza della rete informatica comunale.

Rilevato inoltre che il ruolo di amministratore di sistema attribuito alla ditta GFC comporta per il legale rappresentante Dott. Crippa Gianfranco l'assunzione delle responsabilità civili già previste per i responsabili del trattamento dei dati, a cui l'operato dell'amministratore di sistema è assimilato;

Visto il documento programmatico per la sicurezza come aggiornato nelle risultanze di cui all'allegato, redatto dal suddetto Amministratore di Sistema del Comune di Osnago e ritenuto meritevole di approvazione;



COMUNE DI OSNAGO

PROVINCIA DI LECCO

Viale Rimembranze, 3 - Tel. 039952991 - Fax 0399529926
Codice Fiscale 00556800134

Acquisito il parere di cui all'art. 49 - comma 1 del T.U.E.L. - D.Lgs n. 267/2000;

Con voti favorevoli unanimi espressi nei modi e nelle forme di legge;

DELIBERA

1. Di approvare, per le motivazioni espresse in narrativa, l'unito "Documento programmatico - piano operativo per l'adozione delle misure di sicurezza nel trattamento dei dati personali, ai sensi del D.Lgs. 196/03", aggiornato al 31.3.2011;
2. Di dare atto che il titolare provvederà a riferire, nella relazione accompagnatoria del prossimo bilancio d'esercizio, dell'avvenuto aggiornamento del documento programmatico sulla sicurezza, in conformità a quanto previsto al punto 26 dell'allegato B al D. Lgs 196/2003;
3. Di dichiarare il presente atto, con separata votazione favorevole, immediatamente eseguibile, ai sensi dell'art. 134 - 4° comma del T.U.E.L. - D.Lgs n. 267/2000.



COMUNE DI OSNAGO

PROVINCIA DI LECCO

Viale Rimembranze, 3 - Tel. 039 952991 - Fax 039 9529926
Codice Fiscale 00556800134

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: DECRETO LEGISLATIVO 196/03 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" - ALLEGATO B: AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA PER L'ANNO 2011

PARERI DI CUI ALL'ART. 49, COMMA 1 DEL T.U.E.L. - D. LGS N. 267/2000

PARERE DI REGOLARITÀ TECNICA

VISTO: FAVOREVOLE

Osnago, li 29.3.2011



IL RESPONSABILE DEL SETTORE

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi dell'art.19 all. B al
D.Lgs 196/2003 "Codice in materia di trattamento dei dati personali"

Introduzione:

Il presente documento riguarda il **piano operativo annuale delle misure di sicurezza** per l'anno in corso, secondo quanto previsto dal D.Lgs 196/2003 "Codice in materia di trattamento dei dati personali", allo scopo di minimizzare i rischi di distruzione, perdita anche accidentale che il trattamento dei dati personali (in particolare quelli sensibili) inevitabilmente comporta.

Contenuti del Documento Programmatico sulla Sicurezza:

Vengono elencati nell'ordine i seguenti criteri:

- A) *Criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;*
- B) *Criteri tecnici ed organizzativi per assicurare l'integrità dei dati trattati senza l'ausilio di strumenti elettronici (in forma cartacea);*
- C) *Criteri tecnici ed organizzativi per assicurare l'integrità dei dati trattati con strumenti elettronici;*
- D) *Sistema di autenticazione informatica per la sicurezza del trattamento dei dati;*
- E) *Elenco dei trattamenti di dati personali, delle banche dati e delle strutture preposte ai trattamenti;*
- F) *Trattamenti all'esterno;*
- G) *Interventi formativi;*



A) CRITERI TECNICI ED ORGANIZZATIVI PER LA PROTEZIONE DELLE AREE E DEI LOCALI INTERESSATI DALLE MISURE DI SICUREZZA, NONCHÉ LE PROCEDURE PER CONTROLLARE L'ACCESSO DELLE PERSONE AUTORIZZATE AI LOCALI MEDESIMI

1. Protezione delle aree e dei locali interessati
 - 1.1. I server sono collocati in un apposito locale (denominato *sala server*)
 - 1.2. La sala server è dotata di:
 - a) Impianto elettrico a norma;
 - b) Gruppo di continuità che permette la regolare chiusura delle operazioni in corso sul server in caso di mancanza improvvisa di energia elettrica;
 - c) allarme antintrusione
 - 1.3. L'accesso alla sala server è limitato ai soli amministratori di sistema o alle persone espressamente autorizzate dagli stessi, per il tempo strettamente necessario allo svolgimento dei compiti eventualmente assegnati (es. manutenzione software e/o hardware del server).
 - 1.4. In assenza del personale autorizzato, la sala server viene mantenuta chiusa a chiave. La chiave è custodita dai Responsabili della sicurezza dei dati e di sistema.

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|---|---|-------------------|
| La porta di accesso al locale server non è sufficientemente resistente agli urti. | Sostituire la porta | 31.12.2011 |
| La climatizzazione (installata nel...) all'interno dei locali che ospitano i tre server, con aggiunta del RACK con switch ed apparati attivi, non è più sufficiente a garantire condizioni ideali di funzionamento del sistema nel periodo estivo. | Sostituire il climatizzatore con apparecchio più potente | 31.5.2011 |
| La temperatura all'interno del locale che ospita l'UPS è eccessivamente elevata. Non si può garantire il regolare funzionamento dell'apparato nel periodo estivo. | La ditta Emerson, fornitrice dell'UPS, ha raccomandato di installare climatizzatore | 31.5.2011 |

B) CRITERI TECNICI ED ORGANIZZATIVI PER ASSICURARE L'INTEGRITÀ DEI DATI TRATTATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (IN FORMA CARTACEA)

1. Conservazione dei dati personali:
 - 1.1. Le banche dati costituite in forma cartacea sono conservate presso i rispettivi uffici comunali in appositi archivi organizzati.
 - 1.2. I documenti contenenti dati personali sono custoditi in armadi ignifughi, dotati di chiusura a chiave in custodia esclusivamente al personale incaricato del trattamento;
2. Conservazione dei dati sensibili:
 - 2.1. Le banche dati contenenti dati sensibili sono conservate in cassaforte di sicurezza ubicata presso l'ufficio segreteria.
 - 2.2. In nessun caso sono riportati dati sensibili su documenti o contenitori esposti alla vista, anche involontaria, di persone non autorizzate.
3. Accesso ai locali
 - 3.1. Ogni ufficio dispone di uno o più accessi comunque dotati di chiusura a chiave. Le chiavi degli uffici sono conservate in locale non accessibile al pubblico.
 - 3.2. Le chiavi di accesso all'ufficio servizi sociali e polizia locale sono custodite esclusivamente dai responsabili, in considerazione del fatto che all'interno dei suddetti locali sono conservati dati sensibili e/o giudiziari.
 - 3.3. L'accesso agli uffici comunali è protetto da allarme antintrusione attivato e disattivato manualmente dal personale e collegato alla centrale dell'istituto di vigilanza. La sede municipale è altresì controllata esternamente dallo stesso istituto due volte ogni notte.
 - 3.4. Al di fuori dei normali orari di apertura al pubblico, l'accesso agli uffici è inibito dalla chiusura automatica (programmata) della porta principale e consentito esclusivamente dall'interno con apertura manuale oppure, dall'esterno, solo al personale comunale in possesso delle relative chiavi.
4. Protezione dei locali
 - 4.1. All'interno della sede municipale sono ubicati in posizione evidente e agevolmente raggiungibile gli estintori antincendio. Il numero e la dislocazione sono conformi alla normativa in materia e la loro efficacia viene semestralmente verificata da ditta incaricata.
 - 4.2. Il piano seminterrato della sede municipale, che ospita l'archivio storico e corrente, è stato "compartimentato" a termini della normativa antincendi con apposite porte REI. All'esterno dell'edificio è inoltre presente un pulsante che permette, in caso di incendio, di togliere energia elettrica all'intera sede municipale. Il locale è altresì dotato di allarme antintrusione.



C) CRITERI TECNICI ED ORGANIZZATIVI PER ASSICURARE L'INTEGRITÀ DEI DATI TRATTATI CON STRUMENTI ELETTRONICI

1. Sicurezza del software

- 1.1. Presso ciascun ufficio è consentita l'installazione esclusiva delle seguenti categorie di software:
 - a) Software commerciale dotato di licenza d'uso (esempio: pacchetti di office automation)
 - b) Software gestionale realizzato specificatamente per l'Amministrazione Comunale dalle ditte specializzate nel settore della P.A. (es: applicativi in uso al personale)
 - c) Software gestionale realizzato specificatamente dagli organi centrali della Pubblica Amministrazione (es. Istat, INPS, Ministeri ..)
- 1.2. L'eventuale installazione di software diversi deve essere preventivamente valutata e autorizzata dai responsabili della sicurezza.
- 1.3. Al fine di prevenire ed evitare la diffusione di virus informatici, il software viene installato solo da supporti fisici originali dei quali è ben nota la provenienza.
- 1.4. I sistemi operativi e i pacchetti MS Office installati su tutti i PC della rete sono dotati di regolare licenza e sono stati uniformati verso Windows XP Professional e MS Office 2003;
- 1.5. Con deliberazione n. 173 del 16.10.2009 è stato approvato dalla Giunta Comunale il "disciplinare interno per l'utilizzo di internet e della posta elettronica da parte dei dipendenti", in conformità a quanto previsto dal Garante per la protezione dei dati personali con il Provvedimento generale pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana – Serie generale n. 58 del 10/03/2007

2. Integrità dei dati

- 2.1. L'amministratore di sistema è il responsabile dell'attivazione e verifica del buon funzionamento delle procedure di backup dei dati conservati sui server.
- 2.2. Sui server Windows 2000 e SBS 2003:
 - a) Il salvataggio dei dati viene eseguito quotidianamente, ad eccezione della domenica, con procedura automatica impostata sul server per iniziare alle ore 23.00.
 - b) I dati vengono salvati su un supporto a nastro che viene inserito manualmente nel drive ogni mattina, a cura del personale. Esiste pertanto una cassetta per ogni giorno feriale.
 - c) I dati salvati riguardano sia dati documentali che banche dati. Restano esclusi di volta in volta software o informazioni non indispensabili. La procedura di backup è configurata in modo da restituire il risultato del salvataggio evidenziando eventuali file non salvati con indicazione dell'anomalia riscontrata.

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|---|--|-------------------|
| La dimensione del supporto di backup del server SBS2003 non è sufficiente a contenere tutte le informazioni disponibili sul server. Di conseguenza, di volta in volta, a fronte di necessità, vengono esclusi ambienti la cui mancanza non impedisce il pieno ripristino delle attività degli uffici in caso di "disaster recovery" | Il previsto passaggio ad una nuova piattaforma di programmi applicativi, determinerà la rimozione dal server SBS2003 di una gran mole di dati. La capacità del nastro di backup dovrebbe quindi ritornare ad essere sufficiente. | 31.12.2011 |
| Non sempre la procedura di backup si conclude correttamente, a causa di un'anomalia nel comportamento del servizio di backup di Microsoft. Nonostante aver approfondito l'esame, il problema | L'anomalia viene evitata utilizzando l'accesso diretto alla cartella di log del backup per la visualizzazione dei rapporti, invece di usare lo strumento | 31.12.2011 |

| | | |
|--|--|--|
| non è stato risolto in maniera diretta. Il problema è stato "aggirato" in maniere efficiente ed efficace | Microsoft. Al termine della migrazione verso i nuovi applicativi (per evitare imprevisti sulle banche dati), si tenterà l'update dell'ambiente Microsoft con la speranza che l'anomalia rientri | |
|--|--|--|

- d) Una volta alla settimana, una copia dei dati viene trasferita nella cassetta di sicurezza situata presso la tesoreria comunale (edificio separato dalla sede municipale).
- e) Le cassette con i salvataggi quotidiani sono conservate in apposito armadio ignifugo ubicato presso l'ufficio segreteria (locale separato dal locale server).
- f) I server sono dotati di un gruppo di continuità che assicura l'alimentazione elettrica in caso di perdita di energia sulla rete

2.3. All'inizio del mese di marzo 2011 è stato installato server Linux destinato ad ospitare i nuovi applicativi per gli uffici comunali (Sicr@web). Il backup, appena avviato, segue la procedura:

- a) Il salvataggio dei dati viene eseguito quotidianamente, ad eccezione della domenica, con procedura automatica impostata sul server per iniziare alle ore 23.00.
- b) I dati vengono salvati su un supporto a nastro che viene inserito manualmente nel drive esterno ogni mattina, a cura del personale. Esiste pertanto una cassetta per ogni giorno feriale.
- c) Il server è dotato di un gruppo di continuità che assicura l'alimentazione elettrica in caso di perdita di energia sulla rete
- d) Le cassette con i salvataggi quotidiani sono conservate in apposito armadio ignifugo ubicato presso l'ufficio segreteria (locale separato dal locale server).

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|---|---|-------------------|
| Il rapporto di backup di Linux restituisce errore attestante l'avvenuta esclusione dal backup dei file in uso dal sistema al momento di avvio del backup. | E' necessario verificare con la ditta fornitrice del software se i file esclusi dal backup sono effettivamente inessenziali per l'eventuale ripristino. | 31.12.2011 |
| Al momento non è ancora conservata presso la cassetta di sicurezza in banca la copia settimanale (e mensile). | La procedura sarà attiva dal momento in cui tutto gli applicativi Sicr@web saranno in funzione. | 31.12.2011 |

2.4 I server ed i client sono protetti da UPS a fronte di mancanza di alimentazione elettrica. L'UPS interviene per un tempo che consente lo spegnimento corretto dei server con procedura automatica;

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|---|--|-------------------|
| L'UPS è di recente installazione (marzo 2011) e la programmazione dei tempi e modalità di | E' necessario installare analogo software sul server Linux | 31.12.2011 |

| | | |
|--|---|--|
| spegnimento automatico sono per ora stati configurati solo sui server SBS2003 e WIN2000 non interviene per lo spegnimento dei client | Durante l'orario di lavoro, l'UPS è in grado di tenere i PC attivi e consentire agli utenti lo spegnimento; durante la notte i PC sono spenti | |
|--|---|--|

2.3. In casi particolari, il backup viene effettuato localmente nell'ambito di taluni uffici. In questo caso l'incaricato effettua le seguenti operazioni:

- a) Esecuzione quotidiana del backup, eventualmente tramite procedure automatiche
- b) Copia del risultato di backup sul server allo scopo di consentirne il salvataggio quotidiano con le modalità di cui ai punti precedenti.

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|--|--|-------------------|
| Alcune banche dati installate direttamente dagli utenti potrebbero essere memorizzate localmente su PC sui quali non è prevista una procedura di backup: rischio di perdita dei dati | Ricognizione degli applicativi in uso presso gli utenti e trasferimento degli archivi su server. Qualora non sia possibile predisporre una procedura automatica per tale salvataggio, si instruiranno gli addetti ad effettuare manualmente una copia su server dell'archivio, con cadenza adeguata alla frequenza di aggiornamento dei dati | 31.12.2011 |

2.5. Ulteriori accorgimenti, disponibili su MS Word e MS Excel, a tutela del trattamento di dati sensibili, consentono:

- a) il salvataggio temporaneo automatico con periodicità inferiore a 10 minuti
- b) il salvataggio eventuale su hard disk del PC con registrazione protetta da password scelta dall'utente
- c) compressione dei dati elaborati in appositi file di tipo ".zip" con password per eventuale invio all'indirizzo e-mail noto e certo (certificato);

2.6. In caso di trattamenti di dati personali affidati all'esterno della struttura (ad es. per manutenzione delle banche dati ad opera della ditta cui è affidata l'assistenza del software) verranno adottati i seguenti criteri da adottare per garantire l'adozione delle misure minime di sicurezza:

- a) Ove possibile, l'invio dei dati avviene in modalità ftp con trasferimento dei dati direttamente sul sito del destinatario in forma compressa e con password;
- b) Se inviati con posta elettronica, i file vengono opportunamente compressi con password ed inviati solo a destinatario certo e, quando possibile, a casella di posta elettronica certificata;
- c) Ad ogni destinatario dei dati viene richiesta apposita dichiarazione in cui viene attestato il rispetto delle disposizioni in materia di sicurezza nel trattamento dei dati;

3. Sistema di monitoraggio:

- a. **ACCESSI DELL'AMMINISTRATORE DI SISTEMA:** A termini di legge (Provvedimento del Garante del 27.11.2008, in vigore dal 1.7.2009), è stato introdotto dal 1.1.2010 il sistema di monitoraggio degli accessi dell'Amministratore di Sistema. Le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le citate registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi.

Il nome "administrator" (utente standard previsto dall'ambiente Microsoft per l'amministrazione dei sistemi e facente capo al dominio), viene usato per scopi amministrativi e sistemistici. E' stato introdotto lo username "crippa" (anch'esso con privilegio di amministratore di dominio) con password riservata, per scopi amministrativi previsti dalla stessa normativa. Tali utenti sono ricondotti all'Amministratore di Sistema nominato dal Titolare del Trattamento dei Dati. Anche sulle postazioni client, l'accesso dell'AdS avverrà con lo username "administrator" di dominio senza più accedere con il profilo "administrator" locale al PC, la cui password rimane a conoscenza del solo responsabile del trattamento dati. Tutti gli accessi sono tracciati in file di log e in un formato non modificabile e conservati per 6 mesi; possono essere ispezionati con un programma ad hoc e vengono salvati in file giornalieri che conservano gli accessi da mezzanotte a mezzanotte. La procedura si conforma alle richieste del garante della privacy per quanto riguarda il monitoraggio del comportamento dell'amministratore di sistema.

- b. **ACCESSI DEGLI UTENTI A INTERNET:** Alla fine del 2010, in conformità alla lettera C punto 1 del "disciplinare interno per l'utilizzo di internet e della posta elettronica da parte dei dipendenti", approvato con deliberazione GC 173/2009, è stato acquistato e installato un proxy configurato in modo che le attività sull'uso del servizio di accesso ad internet vengano automaticamente registrate attraverso i file di log e siano conservate per un periodo di un mese e non oltre

4. Interventi di ripristino dei dati

- 4.1 In caso di necessità, il ripristino dei dati è previsto entro le 24 ore successive all'avvenuta conoscenza della perdita, a cura dei responsabili della sicurezza
- 4.2 Qualora non fosse possibile procedere al ripristino dei dati memorizzati con l'ultimo salvataggio, si procederà al restore dell'ultimo nastro utile. Nella peggiore delle ipotesi verranno ripristinate le banche dati memorizzate sul supporto trasferito nella cassetta di sicurezza. I dati ripristinati non avranno quindi età superiore a 7 giorni

5. Protezione dai rischi di intrusione (Antivirus)

- 5.1. Il server Windows SBS 2003 è dotato di sistema antivirus Eset Nod32 versione 4 che distribuisce ed aggiorna automaticamente le firme dei virus e le protezioni (trojan, dialer, spyware, jokes, altro) ai client della rete.
- 5.2 A maggior garanzia di sicurezza per i dati presenti sul sistema informativo, è stato attivato su piattaforma Linux un firewall (IPCOP 1.4.x aggiornato all'ultima versione disponibile) a protezione dagli accessi non consentiti dall'esterno e da intrusioni di hacker o di ambienti software evoluti capaci di mettere a repentaglio la sicurezza dei dati. L'accesso esterno al firewall, per manutenzione e monitoraggio, è protetto da password e criptato.
- Sui computer è altresì attivo un firewall locale, previsto già sulla piattaforma Microsoft.
- 5.3 Con cadenza settimanale, anche ai fini della normativa in materia di sicurezza legata alla carta di identità elettronica, viene consultato il firewall per rilevare eventuali rischi di intrusione, porvi rimedio ed aggiornare le regole antintrusione.
- 5.4 In caso di segnalazione di rischi di intrusioni probabili e non debellate dal sistema antivirus in uso, viene scaricato ed installato su ogni PC apposito tool tra quelli disponibili su internet.
- 5.5 Il programma antivirus è configurato in modo da procedere alla scansione sia in entrata che in uscita di ogni messaggio di posta elettronica esterna e relativi allegati, integrandosi con Exchange. Outlook è altresì in grado di bloccare messaggi in transito sulla posta elettronica interna qualora rilevi la possibile "inattendibilità" di detti allegati. L'antispamming è gestito direttamente da MS Outlook, che utilizza il proprio filtro per destinare lo spam nella casella di "posta indesiderata" (autolearning).

6. Prevenzione della vulnerabilità degli strumenti (patch)

6.1. Gli aggiornamenti dei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti sono effettuati automaticamente

6.2. La connessione ad internet costantemente attiva su tutti i PC consente di scaricare in tempo reale le patch messe a disposizione da Microsoft e dalla ditta produttrice del software applicativo in uso:

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|---|---|-------------------|
| La segnalazione automatica di disponibilità di aggiornamenti che compare sui video dei client, necessita di essere espressamente accettata: non tutti gli utenti sono stati sensibilizzati sulla necessità di confermare l'installazione degli aggiornamenti. | Istruzione degli addetti affinché procedano tempestivamente e correttamente all'installazione degli aggiornamenti proposti dal sistema. | 30.6.2010 |



D) SISTEMA DI AUTENTICAZIONE INFORMATICA PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

1. Controllo degli accessi

- 1.1. L'accesso alla rete di sistema può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password ("credenziali di autenticazione");
- 1.2. Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato "profilo", rispetto alle risorse del sistema informatico. A ciascun profilo è associato un gruppo di utenti, che condividono gli stessi privilegi di accesso ed utilizzo;
- 1.3. Fin nel dettaglio delle voci di menu delle diverse applicazioni, ad ogni nome utente sono associati diversi livelli di accesso (nessuno, sola lettura, modifica), così da limitare in maniera trasparente, intuitiva e sicura la visibilità e la modifica delle banche dati;
- 1.4. Gli applicativi relativi ai servizi demografici e finanziari disciplinano inoltre ad un ulteriore livello l'accesso degli utenti in modalità sola lettura, abilitando alla modifica dei dati unicamente il personale responsabile dei relativi trattamenti;
- 1.5. Gli applicativi utilizzati per il trattamento dei dati possono sfruttare l'autenticazione di cui al punto 1.1, oppure richiedere a loro volta un nome utente e/o una password
- 1.6. Il nome utente non può essere assegnato ad altri incaricati, neppure in tempi diversi
- 1.7. Gli amministratori provvedono, con cadenza almeno semestrale, alla verifica degli elenchi degli utenti ed alla disattivazione delle utenze:
 - a) Non utilizzate da oltre sei mesi (a meno che trattasi di credenziali preventivamente autorizzate per soli scopi di gestione tecnica);
 - b) Che abbiano perso le qualità che consentono all'incaricato l'accesso ai dati personali;

2. Accesso remoto da parte di utenti

- 2.1 Per esigenze di manutenzione, è stata attivata una funzionalità di assistenza remota da parte di personale accreditato (es. amministratore di sistema; ditte produttrici degli applicativi, fornitori) in modalità protetta e dove richiesto, crittografata.

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|---|--|-------------------|
| L'accesso da remoto da parte di alcuni fornitori di applicativi avviene con lo strumento UltraVNC Server che al momento viene utilizzato in modalità non criptata | Individuare uno strumento che consenta ai fornitori di accedere da remoto in modalità esclusivamente criptata. Si è concordato per la migrazione da un server windows al nuovo server LINUX anche un accesso tramite una VPN che risolve per certi aspetti la situazione | 30.9.2010 |

- 2.2 Gli utenti della Polizia Locale sono abilitati ad accedere in modalità remota da un PC situato presso il comune di Lomagna (convenzionato) in modalità protetta e criptata terminal server, aprendo una connessione VPN. A maggior protezione delle banche dati, gli applicativi ed i dati della polizia locale sono stati isolati sul solo server Windows 2000.

3. Password

- 3.1. Una volta accesa la macchina, viene richiesto l'inserimento del nome utente e di password. Il nome utente è preconfigurato per delimitare l'ambito di accesso dell'utente così connesso ai diversi ambienti della rete aziendale (dalla posta elettronica all'accesso a cartelle condivise);
- 3.2. Le password di accesso alla rete e di accesso agli applicativi:

- a) Non devono derivare dal nome utente o dai dati personali dell'utente né contenere riferimenti agevolmente riconducibili all'incaricato;
 - b) Devono avere lunghezza minima di otto caratteri oppure, qualora lo strumento non lo permetta, da un numero da caratteri pari al massimo consentito; devono essere alfanumeriche con caratteri sia minuscoli che maiuscoli.
 - c) Sono strettamente personali: l'utente è tenuto a non comunicarle a terzi ed a non annotarle in vicinanza della propria postazione di lavoro o comunque in luoghi incustoditi;
- 3.3. Le password hanno scadenza trimestrale: il sistema invita automaticamente l'utente a modificare la propria password. Tale scadenza temporale è applicata anche per le password di accesso agli applicativi che consentono la configurazione di tale automatismo (Sicra, Polcity).

| CRITICITÀ: | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|--|---|-------------------|
| Non si ha la certezza che le password di accesso agli applicativi abbiano le caratteristiche (lunghezza minima, caratteri alfanumerici ecc) previste dalla legge | Ricognizione delle password in utilizzo e sensibilizzazione degli utenti in merito; contattare i fornitori per richiedere piena adempienza alla legge | 1.7.2011 |
| E' possibile che i fornitori degli applicativi abbiano conoscenza delle credenziali per l'accesso da remoto con diritti di amministratore | Fornire le credenziali autorizzando l'accesso di volta in volta e senza rendere note le credenziali. | 1.7.2011 |

3.4. Le password non possono essere assegnate ad altri incaricati, neppure in tempi diversi.

4. Copie delle credenziali

- 4.1. La custodia delle copie delle credenziali si rende necessaria esclusivamente qualora l'accesso ai dati ed agli strumenti elettronici sia consentito esclusivamente mediante uso di password non gestibili né dall'utente né dagli amministratori di sistema (es: "quantità di informazione" per INA-SAIA, assegnate dal Ministero dell'Interno e non modificabili).
- 4.2. Per le restanti password, la procedura prevede che a fronte della perdita della password da parte dell'utente o a fronte della necessità di intervento da parte dell'amministratore, quest'ultimo è in grado di modificare la password di accesso, di assegnare una password "di cortesia" e di imporre al sistema la richiesta di una nuova password per l'accesso successivo. Viene in tal modo superata la necessità per gli amministratori di disporre di copia delle password degli utenti.

5. Individuazione dei rischi

- 5.1. I responsabili della sicurezza dei dati e del sistema informativo provvedono ad informare tempestivamente i responsabili del trattamento dati di ogni eventuale problema di sicurezza di cui dovessero venire a conoscenza;
- 5.2. I soggetti responsabili del trattamento provvederanno di conseguenza, anche per tramite dei responsabili della sicurezza, a informare tempestivamente gli incaricati:
 - a) della presenza di virus negli elaboratori dell'ufficio;
 - b) di prassi da parte del personale non conformi alle disposizioni di sicurezza;
 - c) della periodica necessità di variazione delle parole chiave da parte degli incaricati;
 - d) della disponibilità di programmi di aggiornamento relativi all'antivirus;
 - e) della perdita delle qualità che consentono all'incaricato l'accesso ai dati personali
- 5.3. I responsabili del trattamento, in caso di necessità, provvederanno ad organizzare iniziative per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza.

F) TRATTAMENTI DI DATI AFFIDATI ALL'ESTERNO

Per l'esercizio delle proprie attività istituzionali, il Comune può affidare a terzi funzioni o servizi che contemplano necessariamente il trattamento di dati personali, sensibili e/o giudiziari.

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 al Codice per il trattamento dei dati personali;
2. di ottemperare agli obblighi previsti per la protezione dei dati personali;
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrando le procedure già in essere
4. di aver adottato il Documento Programmatico della Sicurezza (in caso di trattamenti effettuati tramite strumenti elettronici) previsto dal D.Lgs 196/2003
5. di impegnarsi a relazione annualmente sugli aggiornamenti apportati al suddetto DPS.
6. di riconoscere il diritto del Comune a verificare periodicamente l'applicazione delle norme di sicurezza adottate

Nella tabella sono riportati gli impegni allo stato attuale contrattualmente assunti e per i quali è già stato emesso provvedimento di nomina a responsabile del trattamento:

| ATTIVITÀ' | DESCRIZIONE DEL TRATTAMENTO | DATI PERSONALI | DATI SENSIBILI / GIUDIZIARI | SOGGETTO |
|------------------------------------|--|---|--|--------------------------------------|
| MANUTENZIONE E ASSISTENZA SOFTWARE | Manutenzione ed assistenza del software applicativo in uso presso il Comune | Tutti i dati contenuti nelle banche dati del sistema informativo comunale | Tutti i dati contenuti nelle banche dati del sistema informativo comunale | SAGA SPA di Orzinuovi (BS) |
| MANUTENZIONE E ASSISTENZA SOFTWARE | Manutenzione ed assistenza del software applicativo in uso presso l'ufficio Polizia Locale | Tutti i dati contenuti nelle banche dati del sistema informativo comunale | | OPEN SOFTWARE SRL di Mirano (VE) |
| ASSISTENZA SOFTWARE | Assistenza del software applicativo per la gestione delle retribuzioni | Tutti i dati contenuti nelle banche dati del sistema informativo comunale | Riferiti al personale dipendente (Rilevazione assenze e permessi per malattie, aspettative, rappresentatività sindacali, visite mediche di idoneità, denunce di infortunio sul lavoro, trattenute per adesioni sindacali e per scioperi (salute); opinioni sindacali, religiose, filosofiche, politiche; abitudini sessuali). Emolumenti per familiari (salute). | MCP ITALIA di Porto San Giorgio (AP) |
| MANUTENZIONE E ASSISTENZA | Manutenzione ed assistenza del | Tutti i dati contenuti nelle | | STARCH srl di Ornago (MI) |

| | | | | |
|--|---|---|--|--|
| SOFTWARE UTC | software applicativo in uso presso l'ufficio tecnico comunale | banche dati del sistema informativo comunale | | |
| CONSULENZA SISTEMA INFORMATIVO COMUNALE | Manutenzione del software | Tutti i dati contenuti nelle banche dati del sistema informativo comunale | Tutti i dati contenuti nelle banche dati del sistema informativo comunale | GFC srl di Osnago |
| TESORERIA COMUNALE | Tenuta e gestione della tesoreria comunale | Anagrafe creditori/debitori del Comune | | Credito Valtellinese di Sondrio |
| MENSA SCOLASTICA | Gestione del servizio di somministrazione pasti agli alunni, insegnanti, dipendenti comunali presso gli istituti scolastici | Nominativi degli utenti | Dati sulla salute, sulle convinzioni religiose di utenti con particolari necessità dietetiche. | Punto Ristorazione srl di Gorle (BG) |
| PUBBLICHE AFFISSIONI | Gestione servizio affissione negli spazi pubblici e riscossione della relativa imposta | Anagrafica degli utenti | Dati giudiziari per la riscossione coattiva | AIPA spa di Milano |
| RISCOSSIONE RUOLI COATTIVI | Riscossione somme a ruolo per TIA e sanzioni codice della strada | Anagrafica dei contribuenti | Dati giudiziari per la riscossione coattiva | SO.GE.R.T. spa di Grumo Nevano (NA) |
| VISITE MEDICHE D.LGS 626/94 | Controlli medici periodici e visite preassunzione del personale comunale | Dati del personale comunale | Dati relativi alla salute | Economie Ambientali di Lecco |
| SERVIZIO ASSISTENZA DOMICILIARE | Fornitura di personale ausiliario per servizio assistenza domiciliare | Dati anagrafici utenti del servizio | Dati relativi alla salute, convinzioni religiose, abitudini sessuali | RETESALUTE Az. Speciale Consortile di Merate |
| SERVIZIO ASSISTENZA EDUCATIVA | Fornitura di personale educativo rivolto a minori, nuclei familiari, soggetti rischio emarginazione | Dati anagrafici utenti del servizio | Dati relativi alla salute, convinzioni religiose, abitudini sessuali | RETESALUTE Az. Speciale Consortile di Merate |
| SERVIZIO ASSISTENZA TRASPORTO SCOLASTICO | Fornitura di personale per la sorveglianza degli alunni durante il trasporto scolastico | Dati anagrafici utenti del servizio | | Coop. Sociale LA COMETA di Casatenovo (LC) |
| SERVIZIO PRESCUOLA | Fornitura di personale per la sorveglianza degli alunni durante il prescuola scuola primaria | Dati anagrafici utenti del servizio | | Coop. Sociale LA COMETA di Casatenovo (LC) |
| TRASPORTO DISABILI E | Servizio con personale volontario | Dati anagrafici utenti del servizio | Dati relativi alla salute | Associazione di Volontariato lo |

| | | | | |
|----------------------------------|--|---|--|-------------------------------|
| ANZIANI | presso centri sociali, sanitari ecc. | | | per Osnago |
| SITO COMUNALE E NEWSLETTER | Manutenzione ed implementazione sito web comunale ed indirizzario newsletter | Anagrafe utenti, associazioni e iscritti alla newsletter | | V.I.P. srl di Oggiono (LC) |



G) INTERVENTI FORMATIVI

1. Gli interventi formativi rivolti agli incaricati del trattamento avranno come contenuti:
 - 1.1. Renderli edotti dei rischi che incombono sui dati e delle misure disponibili per prevenire eventi dannosi;
 - 1.2. I profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
 - 1.3. Le responsabilità che derivano dalla non corretta o insufficiente applicazione delle misure di sicurezza
 - 1.4. Le cautele da adottare per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
 - 1.5. Le istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
2. La formazione è programmata:
 - 2.1. Al momento dell'ingresso in servizio;
 - 2.2. In occasione di cambiamenti di mansioni
 - 2.3. In occasione dell'introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
3. Ogni anno vengono programmate modalità ed entità dell'intervento formativo che può consistere in:
 - 3.1. Giornate di studio o seminari destinati collettivamente agli incaricati ed ai responsabili;
 - 3.2. Attività ristrette di formazione per gruppi di utenti;
 - 3.3. Aggiornamenti rivolti ai soli responsabili;
 - 3.4. Divulgazione materiale informativo agli interessati riferito alle novità o migliorie in materia di sicurezza
4. In sede di prima applicazione del presente documento, ai responsabili ed agli incaricati dei trattamenti è stata consegnata copia del "Memorandum in materia di sicurezza nel trattamento di dati personali".
5. Tenuto conto della precedente formazione attuata nel 2003, 2004 e 2005 a favore di tutto il personale comunale, anche per l'anno 2011, come per il 2006, 2007, 2008 e 2009, la formazione sarà programmata ai sensi del precedente punto 2 e verrà assicurata dal referente interno dell'ente in materia di privacy.



E) Elenco dei trattamenti di dati personali, delle banche dati e delle strutture preposte ai trattamenti

Vengono qui indicate le strutture che costituiscono i diversi settori ed uffici del Comune di Osnago.

Per ogni trattamento sono evidenziate le criticità specifiche, intendendosi le criticità riportate all'interno delle restanti sezioni del Documento programmatico come COMUNI a tutti i trattamenti.

Gli incaricati del trattamento di seguito elencati sono tutti nominati con provvedimento del titolare, così come i responsabili del trattamento i cui nominativi sono riportati specificatamente per ogni settore / servizio.



SETTORE 1 AMMINISTRATIVO, CONTABILE E SERVIZI ALLA PERSONA

Servizi Demografici – Responsabile del trattamento dati: ROSSI RICCARDINA

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi dei rischi specifici sulle banche dati | Misure da adottare |
|--|-------------------------------------|---|--|---|---|---|
| STATO CIVILE | Frigerio Debora Rossi Riccardina | Rilascio certificati, variazioni dello status del cittadino, scioglimento matrimonio, certificazioni di eseguite pubblicazioni matrimoniali. Permessi di seppellimento posteriori al 2000. | I registri relativi agli atti di nascita, di cittadinanza, di matrimonio e di morte nonché i relativi fascicoli e statistiche contengono dati sensibili relativi: stato di salute, interdizione e tutela; appartenenza razziale o etnica; disconoscimento e riconoscimento, adozioni e affiliazioni, sesso e cambiamento di sesso, convinzioni religiose. Nei fascicoli allegati alle sentenze di divorzio o di nullità ecclesiastica sono compresi anche tutti gli altri dati sensibili previsti dalla legge. Dati giudiziari. Permessi di seppellimento anteriori al 2000 (salute) | <u>CARTACEE:</u> Registri s.c. <u>INFORMATIZZATE:</u> B.D. Stato civile | I registri di stato civile dell'anno in corso sono conservati presso l'ufficio, in vista e accessibili a chiunque (rischio di furto e danneggiamento) | Dotare l'ufficio di armadio con chiusura a chiave in cui custodire i registri |
| SERVIZIO ANAGRAFE | Frigerio Debora Rossi Riccardina | Rilascio certificati, variazioni dello status del cittadino, movimento della popolazione. Visi, permessi, attestazioni, autorizzazioni finalizzate alla disciplina della cittadinanza, immigrazione, asilo, condizione di profugo e rifugiato. Carte d'identità e certificati minori validi per l'espatrio. Rilevazione dati popolazione, edifici, industria a fini statistici | I registri anagrafici contengono dati sensibili inerenti a: cambiamento di sesso, disconoscimento/riconoscimento di filiazione, adozioni internazionali, nazionali e affiliazioni, convinzioni religiose, interdizioni, inabilitazioni, tutele. Gli archivi degli italiani residenti all'estero e i relativi fascicoli contengono dati sensibili relativi a: causa di morte, disconoscimento e riconoscimento di filiazioni, adozioni e affiliazioni, interdizione e inabilitazione, sesso e cambiamento di sesso | <u>CARTACEE:</u> Cartellini carte identità <u>INF. E CARTACEE:</u> B.D. popolazione residente B.D. AIRE B.D. stranieri | | |



| | | | | | | |
|---------------------|-------------------------------------|--|--|---|---|--|
| SERVIZIO ELETTORALE | Frigerio Debora Rossi Riccardina | Gestione elettorato attivo/passivo, sottoscrizione proposte di referendum, | Gli archivi elettorali e i relativi fascicoli contengono dati sensibili relativi all'interdizione e cause ostative previste dalle norme elettorali e riabilitazione degli elettori, impedimenti per scrutatori e presidenti di seggio e giudici popolari, disconoscimento e riconoscimento di affiliazioni, adozioni, eleggibilità amministratori (opinioni politiche) e dati contenuti nel casellario giudiziale(giudiziar). Dati sulla salute rinvenibili nei certificati medici presentati dagli scrutatori in caso di indisponibilità | <u>CARTACEE:</u> Fascicoli e tessere elettorali <u>INF. E CARTACEE:</u> Liste sezionali e generali Incarichi elettorali | I fascicoli e le tessere elettorali sono conservati in armadi chiusi a chiave ma presso altro ufficio comunale, per esigenze di spazio. Nessun rischio di perdita, distruzione o visione non autorizzata ma solo esigenze organizzative e di completezza dei dati | Prevedere il trasferimento della banca dati presso l'uff. anagrafe in armadio idoneo munito di serratura la cui chiave rimane custodita dagli incaricati |
| UFFICIO LEVA | Frigerio Debora Rossi Riccardina | Tenuta liste di leva, ruoli matricolari | Gli archivi di leva militare contengono dati sensibili relativi a: situazioni familiari che determinano la dispensa di leva (salute, Dati giudiziari) Permessi di seppellimento anteriori al 2000. (salute) | <u>INF. E CARTACEE:</u> Liste di leva Ruoli matricolari | | |
| SERVIZI CIMITERIALI | Frigerio Debora Rossi Riccardina | Verbali relativi a esumazioni, estumulazioni, inumazioni, concessioni cimiteriali. Permessi di seppellimento posteriori al 2000. | Permessi di seppellimento anteriori al 2000. (salute) | <u>CARTACEE:</u> Contratti cimiteriali | | |

SETTORE 1 AMMINISTRATIVO, CONTABILE E SERVIZI ALLA PERSONA

Servizio Affari Generali – Responsabile del trattamento dati: PIGAZZINI LUCA

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi dei rischi specifici sulle banche dati | Misure da adottare |
|--|------------------------------------|---|---|--|--|--------------------|
| SEGRETERIA GENERALE | Marco Branchini Giulia Bonanomi | Esercizio del mandato degli organi. Documentazione attività istituzionale. Designazione e nomina rappresentanti in commissioni, enti ed uffici. Attività di assemblee rappresentative, commissioni, organi collegiali. Attività politiche di indirizzo, di controllo e sindacato ispettivo Diritto di accesso agli atti di gara. | Consultazioni elettorali e verifica regolarità (opinioni politiche). Accertamento cause ineleggibilità, incompatibilità, decadenza, rimozione, sospensione, scioglimento organi. (opinioni politiche, dati giudiziari). Esame segnalazioni, petizioni, appelli. (opinioni politiche). Iniziativa popolare e referendum (dati giudiziari ed opinioni sindacali) Dati sensibili e giudiziari riguardanti mozioni, ordini del giorno, risoluzioni, interrogazioni e interpellanze Verifica antimafia. (dati giudiziari) Verifica possesso requisiti dichiarati in sede di gara. (dati giudiziari) Aggiudicazione e stipula contratti. (dati giudiziari) | <u>INFORMATIZZATE:</u> B.D. dei consiglieri B.D. partecipanti gare d'appalto B.D. indirizzi istituzionali Albo associazioni <u>INF. E CARTACEE:</u> B.D. componenti consulte B.D. Verbali deliber. GC/CC B.D. determinazioni dirigenziali B.D. appalti aggiudicati <u>CARTACEE:</u> B.D. contratti, convenzioni e scritture private Albo annuale beneficiari contribuiti | | |
| | | Valutazione bilancio economico e consuntivo, determinazione ed assegnazione contributi ad enti ed associazioni. Difesa degli interessi dell'ente nell'ambito della tutela dei diritti soggettivi e legittimi in sede legale. | Opinioni religiose, politiche, sindacali, filosofiche desumibili dagli Statuti e dalla documentazione trasmessa dalle Associazioni. Tutti i dati sensibili e giudiziari (i dati | | | |

| | | | | | | |
|-------------------------------------|------------------------------------|--|--|---|--|--|
| PROTOCOLLO | Marco Branchini Giulia Bonanomi | Gestione della corrispondenza in partenza ed in arrivo. | riguardano ogni fattispecie che possa dare luogo ad un contenzioso). Gestione della corrispondenza in partenza ed in arrivo (potenzialmente, tutti i tipi di dati sensibili ed i dati giudiziari). | CARTACEE: Registri protocollo INFORMATIZZATE: Protocollo dal '97 Mittenti/destinatari | | |
| ARCHIVIO | Marco Branchini Giulia Bonanomi | Ricerca dati con accesso all'archivio comunale | Ricerca dati con accesso all'archivio comunale (potenzialmente, tutti i tipi di dati sensibili ed i dati giudiziari (i dati riguardano ogni fattispecie che possa dare luogo ad istanze rivolte al difensore civico). | CARTACEE: Archivio storico e corrente | | |
| DIFENSORE CIVICO | Marco Branchini Giulia Bonanomi | Garantire il diritto di imparzialità e di buon andamento della amministrazione. Verifica della legittimità dell'attività amministrativa tramite eventuale controllo degli atti dell'ente (deliberazioni). | Potenzialmente tutti i dati | Potenzialmente tutte le banche dati, sia cartacee che informatizzate | | |
| SPORT, CULTURA, TEMPO LIBERO | Marco Branchini Giulia Bonanomi | Riconoscimenti, premiazioni. Adesione a comitati d'onore, cerimonie e manifestazioni istituzionali. Divulgazione e diffusione delle attività promosse. | Concessione patrocini e autorizzazione utilizzo spazi comunali (Opinioni religiose, politiche, sindacali, filosofiche desumibili dalla documentazione trasmessa dai richiedenti). | | | |
| GESTIONE BIBLIOTECA COMUNALE | Barbara Biffi | Iscrizioni alla biblioteca e prestito libri agli utenti. Gestione attività biblioteconomiche, educative e culturali. | I dati sensibili sono trattati in relazione alle informazioni ricavabili dalle richieste relative ai singoli volumi, ai film ovvero ai documenti presi in visione o in prestito. Ulteriori dati sensibili potrebbero essere acquisiti a seguito di colloqui volti ad accertare le esigenze di studio dei richiedenti, che intendano accedere a talune sale riservate per le quali è previsto l'accesso limitato. | INFORMATIZZATE: B.D. Utenti biblioteca comunale | | |
| UFFICIO COMMERCIO | | Licenze commerciali. Rilascio di autorizzazioni ed altri titoli abilitativi. | Certificati del casellario (giudiziar) | CARTACEE: Fascicoli licenze commercio fisso, aree pubbliche, pubblici | | |

SETTORE 1 AMMINISTRATIVO, CONTABILE E SERVIZI ALLA PERSONA

Servizio Assistenza sociale – Responsabile del trattamento dati: MENABALLI SARA

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi dei rischi specifici sulle banche dati | Misure da adottare |
|---|----------------------------|--|--|--|--|---|
| ASSISTENZA SOCIALE E DOMICILIARE | Luca Pigazzini | Gestione delle attività sociali e assistenziali relativi a disabili, famiglie, anziani, extracomunitari, persone con problemi psichici Gestione delle attività socio-assistenziali relative ad anziani e disabili | Documentazione per l'accesso a interventi di sostegno, ricovero, affidi, adozioni, contributi, sussidi, servizio di teleassistenza, centro di terapia riabilitativa e punto prelievi (salute, abitudini sessuali, origine razziale ed etnica). TSO (salute) Dati Giudiziari Gestione del servizio di assistenza domiciliare (salute, dati giudiziari). | <u>INF. E CARTACEE:</u> B.D. assistiti SAD B.D. minori a rischio B.D. disabili (inserimenti diurni e residenziali, trasporto) B.D. anziani bisognosi (buoni sociali, trasporti, teleassistenza, orti, riscaldamento, pasti, case riposo, soggiorni termali) B.D. extracomunitari B.D. contributi (nucleo familiare, maternità, affitto, prima casa) B.D. iscritti centro estivo | Non tutti gli armadi dell'ufficio sono dotati di chiusura a chiave (rischi di accesso non consentito, danneggiamento o sottrazione). | Predisposizione serratura su tutti gli armadi dell'ufficio servizi sociali. |
| ASSEGNAZIONE ALLOGGI EDILIZIA RESIDENZIALE PUBBLICA | Luca Pigazzini | Centro diurno estivo Dati I.S.E.E. per domanda di ammissione ai vari servizi | Certificati medici (salute) Dati I.S.E.E. per domanda di ammissione ai vari servizi (certificati di salute) Predisposizione domanda di assegnazione (giudiziari, salute, origine razziale). | <u>INF. E CARTACEE:</u> B.D. alloggi ERP <u>CARTACEE:</u> Graduatorie ALER Relazioni ASL | | |



SETTORE 1 AMMINISTRATIVO, CONTABILE E SERVIZI ALLA PERSONA

Servizio Tributi ed attività scolastiche – Responsabile del trattamento dati: FUMAGALLI BARBARA

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi dei rischi specifici sulle banche dati | Misure da adottare |
|--|----------------------------|--|--|--|--|---|
| TRIBUTI | Spitale Alessandro | Gestione ruoli TARSU, contravvenzioni codice della strada, tassa pubblicità. Riscossione ICI, TOSAP, IRAP. Applicazione IVA. Redazione mod. 770, mod. Unico. | Applicazione detrazioni ICI (salute). Recupero tasse (dati giudiziari) | INF. E CARTACEE: B.D. tributi (TARSU e ICI) CARTACEE: B.D. Tosap Dichiarazione e prospetti IVA B.D. Affitti e riparto spese alloggi com. Albo provvidenze economiche | | |
| ISTRUZIONE E ATTIVITA' SCOLASTICHE | Spitale Alessandro | Servizio pre-scuola, trasporto scolastico, centri ricreativi, attività parascolastiche. Fornitura libri, sussidi e contributi materiali didattici Appalto del servizio mensa scolastica, gestione iscrizioni e pagamenti, controlli alimentari e igienici. | Interventi educativi formativi di sostegno alla programmazione e per l'inserimento di alunni in difficoltà (salute). Certificazioni e comunicazioni alla ditta appaltatrice relative a diete e regime alimentare (salute, convinzioni religiose, filosofiche o di altro genere) | INF. E CARTACEE: B.D. utenti mensa, trasporto B.D. utenti corso di ruolo B.D. contributi scolastici (libri, trasporto, borse di studio) | Il fax con la comunicazione giornaliera alla ditta di particolari diete (che contiene il nominativo completo dell'utente abbinato al regime dietetico ed alla motivazione religiosa o di salute) rimane esposto alla visione di personale non autorizzato fino al ritiro della ricevuta di trasmissione da parte degli incaricati del trattamento. | L'incaricato provvede a rimuovere la ricevuta di trasmissione contestualmente all'emissione dall'apparecchio fax. |

SETTORE 1 AMMINISTRATIVO, CONTABILE E SERVIZI ALLA PERSONA

Servizio Ragioneria e Personale – Responsabile del trattamento dati: DOTT.SSA MASSIRONI BARBARA

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi dei rischi specifici sulle banche dati | Misure da adottare |
|--|----------------------------------|--|---|---|--|--------------------|
| SERVIZIO PERSONALE E RETRIBUZIONI | Combi Donatella Ponzoni Paola | Verifica requisiti per accesso agli impieghi, comunicazione incarichi esterni. Gestione retribuzioni e pratiche pensionistiche. Iscrizione corsi di formazione | Tenuta fascicoli personali (dati giudiziari). Rilevazione assenze e permessi per malattie, aspettative, rappresentatività sindacali, visite mediche di idoneità, denunce di infortunio sul lavoro, trattative per adesioni sindacali e per scioperi (salute; opinioni sindacali, religiose, filosofiche, politiche; abitudini sessuali). Emolumenti per familiari (salute). | <u>INF. E CARTACEE:</u> B.D. dipendenti B.D. amministratori Statistiche INPDAP <u>CARTACEE:</u> Fascicoli personali dei dipendenti Richieste congedi parentali B.D. rilevazione presenze B.D. Modello 01/M Polizze assicurat. Contratti di lavoro | | |
| SERVIZIO FINANZIARIO, ECONOMICO E PATRIMONIALE | Combi Donatella Ponzoni Paola | Gestione del bilancio di previsione, pluriennale e consuntivo. Attività legate alle spese ed entrate, ai mutui. Gestione dell'inventario e del patrimonio. | Pratiche di sinistri e accertamenti di responsabilità relativamente ad assicurazioni, polizze RCT, equo indennizzo, RC auto, infortuni (salute) | <u>INF. E CARTACEE:</u> B.D. debitori e creditori B.D. albo fornitori Modello 770 B.D. incarichi professionali | | |

SETTORE 2 GESTIONE DEL TERRITORIO E SUE RISORSE

Servizio Gestione del Territorio – Responsabile del trattamento dati: ARCH. MARTUFFO CARMELO

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi dei rischi specifici sulle banche dati | Misure da adottare |
|--|--|---|--|--|--|--------------------|
| PROTEZIONE CIVILE | Pigazzini Paola Tomaghi Marco Targonato Silvia | Attività gestionali e operative per la previsione, prevenzione e pianificazione delle emergenze. | Priorità dettate dalle caratteristiche sanitarie o di disagio psicologico degli abitanti (salute) | | | |
| AMBIENTE ED ECOLOGIA | Pigazzini Paola Tomaghi Marco Targonato Silvia | Autorizzazioni allo scarico in pubblica fognatura; ritiro denunce acque industriali conferite nella rete fognaria. Interventi su segnalazioni e relazioni di sopralluogo. | | CARTACEE: B.D. insediamenti produttivi e ai fini L. 319 | | |
| EDILIZIA PRIVATA ED URBANISTICA | Pigazzini Paola Tomaghi Marco Targonato Silvia | Gestione pratiche edilizie e di occupazione suolo pubblico; espropriazioni; abusi edilizi. | Istruttoria pratiche richiesta contributo regionale per abbattimento barriere architettoniche (salute) | INF. E CARTACEE: Pratiche edilizie Pratiche di condono edilizio CARTACEE: Certificazioni varie | | |
| SPORTELLO UNICO ATTIVITA' PRODUTTIVE | Pigazzini Paola Tomaghi Marco Targonato Silvia | Gestione pratiche edilizie per attività produttiva. | | INFORMATIZZATE: La banca dati è fisicamente ubicata su sito web del polo catastale (accesso con password) | | |
| LAVORI PUBBLICI | Pigazzini Paola Tomaghi Marco Targonato Silvia | Verifica possesso requisiti dichiarati in sede di gara Aggiudicazione e stipula contratti. Diritto di accesso agli atti di gara | Verifica antimafia (giudiziari) | INFORMATIZZATE: SAL opere progettate all'interno UTC B.D. partecipanti a gare in economia CARTACEE: SAL opere progettate all'esterno | | |

SETTORE 3 POLIZIA LOCALE

Responsabile del trattamento dati: GALBUSERA GABRIELE

(I trattamenti da parte di forze di polizia è altresì disciplinato dal Titolo II del D.Lgs 196/2003)

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi del rischi specifici sulle banche dati | Misure da adottare |
|--|--|--|--|---|--|--|
| POLIZIA LOCALE. POLIZIA GIUDIZIARIA, PUBBLICA SICUREZZA | D'Andrea Marco Villa Annamaria Papini Ronny Fumagalli Carlo | Pratiche per accesso a zone a traffico limitato. Tutela dell'ordine e della sicurezza pubblica. Applicazione delle norme in materia di sanzioni amministrative e di codice della strada. Autorizzazione per l'esercizio del mestiere di autonoleggio con conducente | Pratiche relative ad incidenti stradali, denunce di infortunio sul lavoro, contrassegni per invalidi (salute; dati giudiziari), TSO (salute). Prevenzione, accertamento e repressione di reati (giudiziali). Comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia (giudiziali). Autorizzazioni occupazione suolo pubblico da parte di associazioni o partiti (opinioni politiche). Autorizzazioni manifestazioni politiche e religiose (opinioni politiche, sindacali, convinzioni religiose e filosofiche). | INF. E CARTACEE: Verballi violazioni al C.D.S. B.D. cessioni di fabbricato B.D. incidenti stradali B.D. denuncia infortuni sul lavoro Autorizzazioni temporanee polizia amministrativa <u>INFORMATIZZATE:</u> B.D. permessi invalidi Registro agenzie d'affari Registro ascensori <u>CARTACEE:</u> B.D. extracomunitari Registro verbal fermi, sequestro e custodia Fascicoli ascensori Fascicoli agenzie d'affari Registro attività artigianali | | |
| UFFICIO DEL MESSO NOTIFICATORE | Fumagalli Carlo D'Andrea Marco Papini Ronny Villa Annamaria | Tenuta dell'albo pretorio comunale Notificazione atti. | Notifica di atti agli interessati. (giudiziali) | <u>CARTACEE:</u> Registro atti notificati-pubblicati | | Già previste dalla normativa (art. 174 del D.Lgs 196/2003) |

SEGRETARIO COMUNALE/DIRETTORE GENERALE

Responsabile del trattamento dati: ROSA DOTT.SSA RENDA

| Ufficio preposto al trattamento dei dati | Incaricati del trattamento | Trattamenti di dati personali | Trattamenti di dati sensibili e/o giudiziari | Formato delle banche dati | Analisi dei rischi specifici sulle banche dati | Misure da adottare |
|--|----------------------------|---|---|----------------------------|--|--------------------|
| SEGRETARIO COMUNALE DIREZIONE GENERALE | | Attività di assistenza giuridico amministrativa di cui all'art. 97 del T.U. 267/2000 e nello svolgimento delle funzioni di Direttore generale di cui all'art. 108 del T.U. 267/2000 | Funzioni di controllo e di riscontro ed ispettive nei confronti di altri soggetti. Potenzialmente tutti i dati giudiziari e sensibili (i dati riguardano ogni fattispecie oggetto della verifica della legittimità e del buon andamento dell'imparzialità dell'attività amministrativa nonché rispondenza di detta attività ai requisiti di razionalità, economicità, efficienza ed efficacia). | CARTACEE INFORMATIZZATE | E | |





COMUNE DI OSNAGO

PROVINCIA DI LECCO

Viale Rimembranze, 3 - Tel. 039952991 - Fax 0399529926
Codice Fiscale 00556800134

Letto, confermato e sottoscritto

IL SINDACO
Dott. Paolo Sina



IL SEGRETARIO GENERALE
Renda Dott.ssa Rosa

REFERTO DI PUBBLICAZIONE 267

Si attesta che la presente deliberazione è stata pubblicata, in data odierna, per rimanervi per 15 giorni consecutivi nel sito web istituzionale di questo Comune accessibile al pubblico (art. 32, comma 1 della legge 18 giugno 2009, n. 69).

Osnago, li



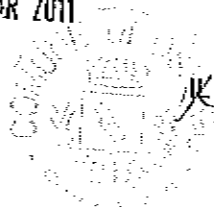
IL RESPONSABILE DEL PROCEDIMENTO

Luca Pigazzini

ESECUTIVITA'

La presente deliberazione è divenuta esecutiva ai sensi dell'art. 134 del T.U.E.L. - D. Lgs. 18 agosto 2000 n. 267 in data

29 MAR 2011



IL RESPONSABILE DEL PROCEDIMENTO

Luca Pigazzini