ALLEGATO ALLA DELIBERA
DI G. C. N. 24 DEL 28/3/2012

IL SEGRETARIO COMUNALE
Dott.ssa M. Bernadette Padula

DISCIPLINARE TECNICO SUL TRATTAMENTO DEI DATI CON STRUMENTI ELETTRONICI: MISURE MINIME DI SICUREZZA –

DECRETO LEGISLATIVO 196/2003 (allegato B)

Approvato con delibera della Giunta Comunale n°_____ del __/__/_____

SOMMARIO:

A) Trattamento dei dati con strumenti elettronici

1) Struttura del sistema e protezioni

- 1.1 Architettura della rete
- 1.2 Sicurezza della rete
- 1.3 Architettura del Sistema Informatico
- 1.4 Sicurezza dei dati

2) Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni

- 2.1 Incaricati del trattamento informatico
- 2.2 Soggetto preposto alla custodia delle credenziali, alla loro attribuzione,cancellazione, modifica
- 2.3 Trattamento dei dati personali affidati ai lavoratori
- 2.4 Trattamento dei dati personali affidati a soggetti esterni
- 2.5 Modalità di gestione delle password
- 2.6 Disattivazione credenziali per disuso

3) Modalità di gestione delle stazioni di lavoro

- 3.1 Soggetto preposto alla pulizia o recupero delle banche dati su PC
- 3.2 Programma antivirus
- 3.3 Interventi di accesso e manutenzione del PC
- 3.4 Società esterne o professionisti per la manutenzione e l'assistenza
- 3.5 Dismissione delle stazioni di lavoro

4) Salvataggio dei dati

5) Locali

6) Cautele generali

- 6.1 Password
- 6.2 Uso del computer
- 6.3 Custodia dei supporti

7) Quadro riepilogativo delle banche dati e dei relativi codici

B) Documento programmatico sulla sicurezza.

C) Trattamento dei dati senza l'ausilio di strumenti elettronici.

1) Quadro riepilogativo delle misure di sicurezza tecniche per i trattamenti senza strumenti elettronici e dei relativi codici.

Allegati: "A1", "A2", "B", "C",

A) Trattamento dei dati con strumenti elettronici

1) Struttura del sistema e protezioni

1.1 Architettura della rete

Sul territorio comunale c'è una sede principale, definita nodo principale, alla quale sono collegate tutte le altre sedi definite nodi secondari;
I nodi secondari sono i seguenti:
Sede della Polizia Locale, Sede della Pubblica Istruzione, Sede del Cantiere comunale, Sede del Cimitero, Sede di Su Planu (Sportello Anagrafe), Sede della Biblioteca
I nodi secondari sono collegati al nodo principale mediante linee ADSL tramite VPN. Tutti i dipendenti dotati di PC sono quindi collegati alla rete Intranet, dalla quale possono accedere alle applicazioni dell'Ente; i dipendenti autorizzati del nodo principale e del nodo pubblica istruzione accedono ad Internet in un unico punto, filtrati dal sistema di firewall aziendale e le loro macchine sono equipaggiate con antivirus di rete. I dipendenti degli altri nodi secondari accedono ad internet tramite la loro linea ADSL, le loro macchine sono equipaggiate con antivirus locale e sistemi di filtraggio standard in dotazione al S.O.

1.2 Sicurezza della rete

La rete del Comune è connessa all'esterno mediante una linea HDSL e una linea ADSL a monte delle quali un sistema di firewall controlla il traffico dati in base a politiche di sicurezza prestabilite.
L'accesso alla rete comunale avviene tramite autenticazione con nome utente e password secondo le regole di dominio.

1.3 Architettura del Sistema Informatico

a) Banche dati

I dati strutturati delle applicazioni gestionali sono memorizzati in una banca dati centralizzata che contiene:

- Dati anagrafe, stato civile, leva, elettorale
- Dati contabili
- Dati tributari
- Dati urbanistici
- Dati amministrativi (protocollo, delibere, determinazioni)

Altre banche dati centralizzate contengono i dati gestiti dalle seguenti applicazioni:

- Opere pubbliche
- Polizia Locale

Oltre alle banche dati delle applicazioni gestionali esistono archivi documentali non strutturati, residenti sulle stazioni di lavoro e riguardanti:

- Dati amministrativi (decreti di liquidazione, decreti dirigenziali, decreti sindacali)
- Dati sensibili relativi alle attività dei Servizi Sociali
- Dati gestiti dalla Polizia Municipale
- Dati gestiti dalle Opere Pubbliche

b) Posta elettronica.

La posta elettronica viene gestita internamente tramite software open source da un server del nodo principale; ad ogni dipendente è assegnata una casella individuale.

c) I Sistemi di autenticazione.

Attualmente il sistema centralizzato di autenticazione/autorizzazione è quello del Dominio Windows Active Directory utilizzato per autenticare gli utenti che accedono ai computer e alle risorse condivise su rete come: cartelle, stampanti, applicativi.

Le procedure applicative non utilizzano questi sistemi centralizzati, ma possiedono un proprio sistema di autenticazione ed autorizzazione degli utenti.

Per l'accesso ai personal computer del nodo principale e della sede della pubblica istruzione ci si avvale del sistema di autenticazione del Domain Controller. Nei personal computer delle altre sedi l'accesso è subordinato ad autenticazione mediante criteri locali.

Ad ogni singolo utente possono essere assegnate più credenziali, diverse fra loro, a seconda delle procedure applicative alle quali accede.

1.4 Sicurezza dei dati.

a) Banche dati centralizzate

L'accesso ai dati avviene tramite le procedure gestionali che li trattano: all'utente viene richiesta la digitazione di username e password. Queste credenziali sono verificate dalla procedura stessa. Contestualmente viene verificato se l'utente è autorizzato all'utilizzo della funzionalità richiesta.

b) Banche dati ed archivi documentali residenti su P.C.

I PC che contengono banche dati locali o archivi documentali, contenenti dati personali e/o sensibili, sono protetti da credenziali di accesso personali, come precedentemente descritto.

2) Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni

2.1 Incaricati del trattamento informatico

Sono tutti gli operatori dell'Ufficio CED.

2.2 Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica

Preposto alla gestione delle credenziali per l'accesso alle banche dati centralizzate sono gli operatori dell'Ufficio CED che provvedono in prima persona in qualità di amministratori di sistema incaricati dal Sindaco.

Il preposto alla gestione delle credenziali provvede, quando necessario, a fornire al responsabile del trattamento l'elenco aggiornato di tutti coloro che, a qualsiasi titolo, sono autorizzati ad accedere alle banche dati di quell'Area.

Il preposto alla gestione delle credenziali può variare la password degli incaricati, in caso che si renda indispensabile ed indifferibile, per esclusiva necessità di operatività e sicurezza del sistema, dandone pronta comunicazione agli stessi in modo riservato.

Nessuna responsabilità può essere addebitata al preposto alla gestione delle credenziali per eventuali ritardi od omissioni a lui non imputabili nella concessione, revoca o modifica delle autorizzazioni.

2.3 Trattamento dei dati personali affidati ai lavoratori

a) Assegnazione delle credenziali di autenticazione.

Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato (userid) associato ad una parola chiave riservata (password).

In caso di assunzione di un nuovo lavoratore, quest'ultimo, il Direttore d'Area competente o il Responsabile del trattamento dei dati da lui delegato, richiede al preposto alla gestione l'assegnazione della casella di posta elettronica e delle credenziali di autenticazione.

Il preposto alla gestione provvede all'assegnazione della posta elettronica, di userid e della password provvisoria inserendo le credenziali nel dominio e nei programmi applicativi e comunica le credenziali all'utente in modo riservato.

E' a cura del lavoratore sostituire la password provvisoria con quella definitiva.

Può accadere che, per esigenze di servizio, esistano credenziali d'accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori.

Queste credenziali non possono consentire l'accesso a banche dati o documenti contenenti dati personali.

b) Assegnazione delle autorizzazioni

Per poter accedere, a qualsiasi titolo, alle applicazioni ed alle banche dati del Comune occorre essere autorizzati. L'autorizzazione del singolo lavoratore ad accedere alle banche dati del Comune deve essere sempre preceduta dal conferimento dell'incarico al trattamento dei dati da parte del responsabile del trattamento. La competenza alla richiesta, revoca, modifica delle autorizzazioni è del Direttore d'Area di appartenenza del lavoratore il quale può delegarla per iscritto al responsabile delegato.

c) Accesso ad applicazioni e banche dati del Settore di appartenenza.

Il Direttore d'Area di appartenenza/responsabile delegato sulla base dell'incarico conferito al lavoratore, comunica per iscritto, anche via e-mail, al preposto alla gestione delle credenziali a quali banche dati il lavoratore è autorizzato ad accedere.
Il preposto alla gestione delle credenziali abilita il lavoratore alle banche dati di sua competenza e provvede a inoltrare la richiesta ai responsabili applicativi per le relative autorizzazioni.

d) Accesso ad applicazioni e banche dati di altre Aree.

Nel caso che il lavoratore necessiti di accedere a banche dati di un'altra Area, l'incarico dovrà essere dato congiuntamente dal Direttore d'Area di appartenenza e dal Direttore d'Area titolare della banca dati utilizzata.
Una volta conferito l'incarico, il Direttore d'Area di appartenenza/ responsabile delegato richiede per iscritto, anche via e-mail, al preposto alla gestione l'abilitazione del lavoratore alle banche richieste, attestando che il Direttore d'Area titolare della banca dati ne è stato informato Il preposto alla gestione procede con le modalità indicate al paragrafo precedente.

e) Cessazione del rapporto di lavoro

Nel caso di cessazione del rapporto lavorativo, il preposto alla gestione delle credenziali, riceve dall'Area del Personale debita comunicazione contenente il nominativo del lavoratore cessato, ne revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica, e ne informa, per iscritto, anche via e-mail, il responsabile informatico dell'applicazione.
Nel caso di rapporto di collaborazione coordinata e continuativa, di prestazione occasionale, di tirocinio formativo ed in genere in tutti gli altri casi, spetta al Direttore d'Area competente/ responsabile delegato comunicare tempestivamente per iscritto, anche via e-mail, al preposto alla gestione delle credenziali l'avvenuta cessazione del rapporto di lavoro e chiedere la revoca delle relative credenziali e autorizzazioni.
Il preposto alla gestione delle credenziali revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica e ne informa per iscritto, anche via e-mail, il Direttore d'Area competente e il responsabile informatico dell'applicazione.
Prima della cessazione del rapporto di lavoro, il lavoratore deve eliminare dal suo PC i documenti e le e-mail che non siano di interesse dell'Area, autorizzando per iscritto il Direttore d'Area ad accedere ai documenti ed alle e-mail rimanenti.
Il Direttore d'Area/responsabile delegato deve prontamente avvisare il soggetto preposto alla pulizia o recupero delle banche dati di cui al punto 3.1 che provvederà al ritiro della stazione di lavoro o comunque a rendere indisponibili i dati legati al profilo del lavoratore dopo averne trattenuto una copia.
Entro un mese il Direttore d'Area/responsabile delegato può richiedere il recupero delle banche dati e delle e-mail giacenti nella casella di posta disabilitata, esibendo la relativa

autorizzazione del lavoratore. Trascorso tale periodo il preposto provvederà alla eliminazione definitiva dei suddetti dati.

f) Trasferimento del lavoratore

Nel caso di trasferimento di un lavoratore presso un'altra Area, il preposto alla gestione delle credenziali, dopo aver rilevato l'informazione attraverso la Banca dati centralizzata dell'Area del Personale, provvede a revocare tutte le autorizzazioni all'accesso del lavoratore, ad eccezione dell'indirizzo di posta elettronica, e ne informa per iscritto, anche via e-mail, il responsabile informatico dell'applicazione.

Il lavoratore trasferito deve reindirizzare all'Area di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo. Il Direttore d'Area di nuova assegnazione/ responsabile delegato, sulla base del nuovo incarico al trattamento dei dati conferito al lavoratore e delle competenze a quest'ultimo attribuite, provvede a richiedere le nuove abilitazioni, anche relative all'accesso a banche dati di un'altra Area, con le stesse modalità previste nel caso di nuova assunzione.

Nel caso di trasferimento di un lavoratore nell'ambito della stessa Area, il Direttore d'Area/responsabile delegato, sulla base del nuovo incarico al trattamento dei dati conferito al lavoratore e delle competenze a quest'ultimo attribuite, comunica per iscritto, anche via e-mail, al preposto alla gestione delle credenziali le autorizzazioni all'accesso da revocare e le nuove applicazioni, anche relative all'accesso a banche dati di un'altra Area, alle quali il lavoratore è autorizzato ad accedere. Il preposto alla gestione delle credenziali disabilita le autorizzazioni all'accesso da revocare, e per le nuove abilitazioni procede con le modalità previste nel caso di nuova assunzione informandone per iscritto, anche via e-mail, il Direttore d'Area e il responsabile informatico dell'applicazione.

Nel caso che il trasferimento del lavoratore (ad un altro Area o nell'ambito della stessa Area) comporti il contemporaneo trasferimento del PC, il lavoratore è tenuto a consegnare al Direttore d'Area i dati e le e-mail di interesse dell'Area e successivamente a rimuoverli dalla propria stazione di lavoro.

Nel caso invece in cui il trasferimento non comporti il contemporaneo trasferimento del PC, si deve seguire il comportamento previsto per il caso di cessazione del rapporto di lavoro

2.4 Trattamento dei dati personali affidati a soggetti esterni

a) Rapporti con i soggetti esterni.

Sono considerati soggetti esterni tutti quei soggetti che non rientrano nel punto 2.3 (a puro titolo esemplificativo: società, enti, consorzi, professionisti, soggetti pubblici o gestori di pubblici servizi, etc.).

La titolarità del trattamento dei dati resta in capo al Comune. I rapporti tra il Comune e i soggetti esterni sono regolati da apposito contratto/convenzione/concessione. Il Direttore

d'Area contraente nomina il soggetto esterno responsabile del trattamento dei dati secondo l'Allegato A1.
Nel caso in cui l'oggetto del contratto, della convenzione o della concessione comporti l'utilizzazione di applicazioni o banche dati di competenza di più Aree, la designazione del responsabile dovrà essere sottoscritta congiuntamente dal Direttore d'Area contraente e dai Direttori d'Area responsabili delle banche dati interessate.
All'inizio della collaborazione il soggetto esterno responsabile del trattamento fornisce al Direttore d'Area l'elenco degli incaricati al trattamento dei dati da lui nominati, secondo l'Allegato A2.
Il Direttore d'Area/responsabile delegato, comunica per iscritto, anche via e-mail, al preposto alla gestione delle credenziali:

- quali applicazioni l'incaricato è abilitato, richiedendo altresì, se necessario, l'accesso ad Internet e l'utilizzo della posta elettronica;
- la data di scadenza del contratto/convenzione/concessione, se in suo possesso. Nel caso in cui l'abilitazione riguardi banche dati di competenza di più Aree, nella comunicazione il Direttore d'Area contraente dovrà altresì dare atto che i Direttori d'Area interessati sono stati informati della richiesta.

Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità delle credenziali di dodici mesi (o inferiore se la data di scadenza del contratto/convenzione/concessione è antecedente a tale termine).
Scaduto il periodo di validità, le credenziali dell'utente, se non intervengono ulteriori comunicazioni, saranno automaticamente disabilitate.
Qualora il contratto/convenzione/concessione abbia una durata superiore all'anno, il responsabile esterno del trattamento dei dati, al fine di evitare che le credenziali degli incaricati siano automaticamente disabilitate alla scadenza dei dodici mesi, dovrà fornire al Direttore d'Area, due mesi prima della scadenza delle stesse, l'elenco aggiornato degli incaricati.
Il Direttore d'Area/responsabile delegato, trasmetterà al preposto alla gestione delle credenziali il nuovo elenco in sostituzione di quello precedente, comunicando, nel caso che nell'elenco siano presenti anche nuovi incaricati, le applicazioni a cui questi ultimi sono abilitati e richiedendo, se necessario, l'accesso ad Internet e l'utilizzo della posta elettronica.

b) Accesso alle banche dati informatizzate del Comune.

L'accesso alle banche dati del Comune è consentito alle Amministrazioni Pubbliche e ai soggetti gestori o concessionari di servizi pubblici esclusivamente per finalità istituzionali.
L'accesso dovrà avvenire secondo le modalità e nei limiti specificati nella convenzione di cui all'allegato "C" che dovrà essere sottoscritta dai Direttore d'Area Responsabile del

trattamento della banca dati e dal Rappresentante della Pubblica Amministrazione/gestore o concessionario di servizi pubblici.

2.5 Modalità di gestione delle password

Le password utilizzate nei sistemi di autenticazione degli applicativi accessibili via web tramite portale istituzionale sono assegnate dal preposto alla gestione delle credenziali all'atto della creazione delle credenziali stesse e vengono comunicate in forma riservata all'utente che deve provvedere, al primo utilizzo, alla sostituzione della password assegnata con una conosciuta solo dal medesimo.

Il dipendente ha l'obbligo di impostare una password a propria scelta nel rispetto della normativa vigente. Nei sistemi Active Directory è stato impostato un meccanismo automatico di scadenza delle password ogni tre mesi. Qualora l'utente dimentichi la propria password del dominio, dovrà rivolgersi al lavoratore da lui delegato (si veda paragrafo 3.3) o, in alternativa, all'Ufficio CED che provvederà, previa identificazione personale, a fornire una password provvisoria che consentirà di accedere alla procedura di modifica della password ma che dovrà poi essere immediatamente sostituita da una definitiva .

Qualora l'utente sia stato disabilitato per mancato uso delle credenziali per un periodo di almeno sei mesi, la procedura di riattivazione delle credenziali è quella di cui al successivo punto 2.6. Un utente che non sia stato disabilitato può, scaduti i termini di validità della password, modificare la propria password autenticandosi con userid e vecchia password. Ogni incaricato che riceve le proprie password ne è direttamente responsabile.

Fatta eccezione per quanto previsto dal paragrafo 3.3, il lavoratore non deve in alcun modo comunicare le proprie password a persone diverse od altri incaricati; qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente provvedere a modificarla.

2.6 Disattivazione credenziali per disuso.

Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione Il Direttore d'Area/responsabile delegato, qualora ritenga di dover riattivare nuovamente le credenziali dell'utente, dovrà chiedere per iscritto, anche via PRONET, al preposto alla gestione delle credenziali il ripristino delle stesse.

L'utente dovrà rivolgersi all'Ufficio CED che provvederà a fornire in busta chiusa una password provvisoria che consentirà di accedere alla procedura di modifica della password ma che dovrà poi essere immediatamente sostituita da una definitiva.

3) Modalità di gestione delle stazioni di lavoro

3.1 Soggetto preposto alla pulizia o recupero delle banche dati su PC

Preposto alla pulizia o recupero delle banche dati su PC è il Responsabile dell'Ufficio CED che provvederà alla designazione del personale incaricato.

3.2 Programmi antivirus

Su tutti i PC sono installati programmi antivirus che vengono aggiornati periodicamente in modo automatico, tramite l'accesso in rete al Server di gestione antivirus o nel caso di portatili o dei PC delle sedi remote mediante aggiornamenti automatici.
L'antivirus installato sui singoli PC controlla in tempo reale i documenti utilizzati.
Oltre che sulle stazioni di lavoro sono installati sistemi antivirus sui server di posta elettronica e proxy per filtrare la navigazione.
I Server di Gestione Antivirus si aggiornano in modo automatico E' opportuno che l'utente, con periodicità almeno quindicinale, effettui con il software antivirus una scansione completa dei dischi interni della stazione di lavoro.

3.3 Interventi di accesso o manutenzione del PC

a) Richiesta di accesso durante l'assenza del lavoratore.

Il Dirigente del Settore o il responsabile del trattamento può accedere a dati e procedure del PC del lavoratore assente e verificare il contenuto dei messaggi a quest'ultimo indirizzati, a condizione che ciò si renda indispensabile e indifferibile, per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa.
A tale scopo ogni lavoratore deve consegnare ad un altro lavoratore da lui delegato per iscritto una busta chiusa contenente le proprie password, avendo cura di sostituirla ogni volta che esse vengono cambiate. Il lavoratore delegato, su richiesta e alla presenza del Direttore d'Area o del responsabile del trattamento, accede ai dati e alle procedure nonché ai messaggi di posta elettronica del lavoratore assente provvedendo a inoltrare al Direttore d'Area o al responsabile da quest'ultimo indicato quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Dell'attività compiuta è redatto apposito verbale a cura del Direttore d'Area/responsabile che ne informa il lavoratore assente alla prima occasione utile.
Nel caso in cui non sia stato delegato alcun lavoratore oppure nel caso in cui anche il lavoratore delegato non sia presente il Direttore d'Area/responsabile delegato richiede ed autorizza l'intervento dei tecnici dell'Ufficio CED, che ne permettono l'accesso per il tempo necessario. Questo intervento verrà documentato mediante apposito verbale redatto a cura del Direttore d'Area/responsabile delegato e comunicato al lavoratore alla prima occasione utile. Gli interventi dei tecnici dell'Ufficio CED possono avvenire senza conoscere e senza modificare la password del lavoratore, grazie ad una password di servizio custodita dal preposto, secondo le regole tecniche previste dalla legge.

B) Interventi di Manutenzione.

Quando per un PC occorre fare un intervento di manutenzione, ordinaria o straordinaria, sul loco o presso i locali CED, sarà cura del lavoratore concordare modi e tempi di intervento con i tecnici addetti. Se l'intervento necessita dell'accesso al PC con le credenziali del lavoratore, queste, se possibile, saranno inserite dallo stesso e non comunicate al tecnico. Nel caso che il lavoratore non possa presenziare all'intervento, questi comunicherà le proprie credenziali al tecnico e provvederà a modificarle una volta terminato l'intervento

3.4 Società esterne o professionisti per la manutenzione e l'assistenza

Il Direttore dell'Area 9, responsabile dell'Ufficio CED nomina la società che effettua la manutenzione dei sistemi hardware o software responsabile del trattamento dei dati utilizzando l'allegato modello A1) il quale andrà integrato con una specifica assunzione di impegno da parte del nominato stesso al rispetto delle seguenti disposizioni:

a) non effettuare copie né procedere alla eliminazione degli archivi informatici di titolarità dell'Ente detenuti.

b) informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici.

c) richiedere preventivamente l'autorizzazione ai tecnici dell'Ufficio CED nel caso di interventi di assistenza tramite collegamento remoto. Gli stessi tecnici dovranno essere avvisati al termine delle operazioni.

d) usare riservatezza su dati ed informazioni addivenuti in loro possesso.

e) trasmettere al Direttore Area 9, responsabile dell'Ufficio CED, all'inizio della collaborazione e, successivamente, per i contratti di durata superiore all'anno, ogni dieci mesi, l'elenco aggiornato degli incaricati al trattamento.

f) nel caso che gli incaricati, per svolgere la propria attività, necessitino di accedere ad uffici e locali del Comune, informare in ogni caso tempestivamente l'Ufficio CED di ogni revoca e di ogni nuovo incarico conferito.

3.5 Dismissione delle stazioni di lavoro

In caso di dismissione di vecchi PC, il Direttore d'Area che ha in carico la stazione di lavoro deve comunicare al soggetto preposto alla pulizia la presenza di banche dati da recuperare. Il soggetto preposto una volta recuperate le banche dati, conserva la stazione di lavoro per un mese quindi provvede a rendere illeggibili i dischi magnetici prima della rottamazione. I dischi dei PC usati che il Comune cede in comodato d'uso prima della consegna vengono riformattati impedendo l'accesso alle banche dati che vi erano contenute.

4) Salvataggio dei dati

Il salvataggio delle banche dati esistenti sui server è in carico all'Ufficio CED. Sui sistemi centralizzati vengono fatte copie quotidiane delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente. Le copie vengono effettuate su più server residenti l'uno presso l'Ufficio CED e l'altro, di backup, presso una sede remota. L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dagli operatori del CED. Ogni singolo lavoratore è responsabile del salvataggio degli archivi esistenti sul proprio PC. Le banche dati residenti solo sul singolo PC (escludendo pertanto, ad esempio, le banche dati che il lavoratore ha creato per esigenze di funzionalità, quelle di cui esiste una copia cartacea ed in genere, quelle che è possibile ricostruire attingendo ad altre banche dati) sono copiate su supporto elettronico a disposizione del singolo lavoratore. Spetta al Direttore d'Area effettuare periodicamente una verifica sulla presenza di banche dati residenti solo su singolo PC e richiedere all'Ufficio CED il supporto eventualmente necessario per il salvataggio dei dati. Tempi e modalità del salvataggio dei dati trattati, che dovrà avvenire con cadenza almeno settimanale, sono definiti nelle istruzioni impartite dai Direttori d'Area. I supporti contenti le copie di backup effettuate dai singoli utenti, quando non più utilizzati, possono essere archiviati o distrutti, ma non utilizzati per altre tipologie di dati o per la trasmissione all'esterno.

5) Locali

I locali dove risiedono fisicamente i server devono essere dotati di alcuni accorgimenti minimi a garanzia sia della sicurezza fisica dell'hardware sia delle banche dati:

1. chiusura di sicurezza per la porta di ingresso ai locali, ed accesso controllato da videocitofono per i dipendenti autorizzati;
2. stabilizzatore di temperatura per i locali;
3. gruppo di continuità e di stabilizzazione della corrente;
4. cassaforte ignifuga per cassette, dischetti e CD di salvataggio;
5. impianto di rilevamento fumi e spegnimento automatico in caso di incendio, collegato con la sede di una società di sicurezza e pronto intervento;
6. impianto antintrusione collegato con la sede di una società di sicurezza e pronto intervento

Il locale dove risiede la seconda libreria automatizzata deve essere dotato di:

1. chiusura di sicurezza per la porta di ingresso al locale;
2. stabilizzatore di temperatura per i locali;
3. gruppo di continuità e di stabilizzazione della corrente.

6) Cautele generali

6.1 Password

La password deve essere composta da almeno 8 caratteri. Le Password non devono contenere riferimenti agevolmente riconducibili all'incaricato e devono essere modificate almeno ogni tre mesi. I sistemi centralizzati di autenticazione provvedono in modo automatico alla scadenza trimestrale della password. E' responsabilità dell'utente provvedere alla modifica della password del PC almeno ogni tre mesi.

6.2 Uso del Computer

Il Direttore d'Area/responsabile delegato deve impartire le istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro. Se il PC viene lasciato acceso incustodito, l'utente attivo al momento deve essere disconnesso o deve essere attivata la modalità salvaschermo con protezione mediante password.

6.3. Custodia dei supporti

Devono essere impartite, da parte del Responsabile del trattamento, le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti

7) QUADRO RIEPILOGATIVO DELLE BANCHE DATI E DEI RELATIVI CODICI

Codici di riferimento per la classificazione delle banche dati :

Codice	Descrizione	Misure di Sicurezza	Tipologia	Responsabilità
1	Banca dati informatizzata	centralizzata tecnica e organizzativa	Progetti Telematici	Ufficio CED
2	dati residenti su PC	personale	tecnica e organizzativa	Incaricato

Le Determinazioni di specificazione del presente documento dovranno fare riferimento, nelle schede descrittive (allegato "B"), ai codici sopra evidenziati. Qualora per un particolare trattamento i codici siano più di uno, vanno indicati tutti.

B) Documento programmatico sulla sicurezza

Il presente documento, considerate le caratteristiche organizzative dell'Ente, rinvia alcuni adempimenti alle determinazioni che i singoli Direttori d'Area, in quanto titolari del trattamento dei dati, devono adottare e precisamente:

1. l'elenco dei trattamenti di dati personali;

2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati ovvero la nomina dei Responsabili dei trattamenti e degli Incaricati.
3. l'analisi dei rischi che incombono sui dati.
4. Le misure ulteriori da adottare, aggiuntive rispetto a quelle indicate nei seguenti punti 4.1, 4.2, 4.3, 4.4 per garantire l'integrità e la disponibilità dei dati. Altri adempimenti:
   - 4.1 Le misure da adottare per garantire l'integrità e la disponibilità dei dati elettronici, sono state dettagliatamente evidenziate al punto A del presente Disciplinare Tecnico.
   - 4.2 Il Servizio Prevenzione e Protezione, dell'Area Tecnologica, dovrà garantire la protezione delle aree e dei locali, con specifico riferimento ai Piani di Emergenza elaborati per le diverse Strutture Comunali.
   - 4.3 Il Servizio Prevenzione e Protezione, dell'Area Tecnologica dovrà provvedere alle autorizzazioni ad accedere ai locali al di fuori dell'orario di lavoro del personale dell'impresa di pulizia per le sedi oggetto di appalto.
   - 4.4 l'accesso al Palazzo Comunale dopo l'orario di chiusura è garantito dal personale di sorveglianza gestito dall'Area 9 ed anche a mezzo di strumenti di Videosorveglianza degli accessi installati dal Servizio Prevenzione e Protezione, dell'Area Tecnologica.

     L'accesso dopo l'orario di chiusura nel Palazzo Comunale e nelle sedi staccate di uffici comunali: via d'Azeglio (Pubblica Istruzione), Piazza Si 'e Boi (Biblioteca), via Dante (Polizia Locale), Località Bia 'e Mara (Cantiere Comunale e Archivio Storico), Cimitero, Su Planu (Servizi Demografici e Polizia Locale), è consentito ad Amministratori e lavoratori autorizzati in quanto titolari di apposito badge identificativo personale che attiva il dispositivo per l'apertura degli ingressi. L'Area Tecnologica cura la gestione dei sistemi di allarme esistenti nel Palazzo Comunale e nelle sedi staccate suddette.
5. Il Servizio CED in conformità alle disposizioni di legge provvede alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.
6. L'Area 9, Responsabile del CED, dovrà curare la formazione dei dipendenti in modo speciale nei confronti dei nuovi assunti. In modo particolare il programma di formazione dovrà :
   a) rendere consapevoli i partecipanti dell'importanza delle scelte dell'Ente;
   b) coinvolgere i partecipanti sulle problematiche inerenti alla sicurezza;
   c) responsabilizzare i partecipanti sulle attività da eseguire. I corsi saranno progettati in base alle diverse esigenze ed ai diversi sistemi di sicurezza

sviluppati, in funzione al grado di informatizzazione raggiunto; in generale non potranno mancare riferimenti a:

- normativa vigente;
- definizione delle responsabilità;
- elenco delle vulnerabilità: spesso non c'è la consapevolezza dei rischi che si possono correre;
- regole comportamentali che comprendono la gestione degli accessi (password.);
- regole comportamentali di riservatezza sia in orario di lavoro sia al di fuori dell'ambito lavorativo;
- i possibili rischi: virus, intercettazioni, intrusioni, ecc..

7. Ogni Settore provvede:
   - alla conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali trattati per finalità che non richiedono il loro utilizzo;
   - all'adozione di codici identificativi o soluzioni analoghe che rendano i dati sensibili e giudiziari contenuti in elenchi, registri, banche dati tenuti con l'ausilio di strumenti elettronici temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità. Per tale attività le Aree si avvalgono , qualora lo ritengano opportuno, dell'ausilio del Servizio Sistemi Informativi
8. Il Comune è impegnato in un processo di valorizzazione dell'utilizzo della rete telematica, ma è consapevole che tale impegno deve essere attuato nel pieno rispetto delle previsioni normative, dei principi di necessità, pertinenza e non eccedenza dei dati personali, del diritto all'oblio e dei diritti fondamentali della persona. In particolare, sono allo studio ed in via di sperimentazione forme adeguate di selezione dei dati pubblicati sul sito web del Comune che evitino, per quanto possibile, che i comuni motori di ricerca esterni possano, in qualsiasi momento, in modo massivo e indiscriminato, reperire un insieme di dati personali resi disponibili in rete. Sarà pertanto cura di ogni singolo Direttore d'Area individuare, volta per volta, i casi in cui è necessario o opportuno che documenti, atti, informazioni della propria Area, pur rimanendo accessibili attraverso la pubblicazione sul sito web del Comune, vengano trattati con le tecniche più adeguate per escludere selettivamente l'accesso dei motori di ricerca. A tal fine, il Direttore d'Area, nei casi sopra indicati, dovrà concordare con il Servizio Comunicazione e Rapporti con i cittadini dello Staff l'adozione delle misure più opportune alla scopo (attraverso, ad esempio, l'inserimento nella pagina web di opportuni comandi o l'attribuzione alle sole persone interessate di una chiave personale di accesso) In ogni caso, sarà cura del Direttore d'Area individuare il periodo temporale

entro il quale si potrà ritenere proporzionato, in rapporto alle finalità perseguite, mantenere sul sito del Comune documenti, atti, informazioni sia che essi siano direttamente individuabili anche tramite motori di ricerca esterna sia che l'azione dei motori di ricerca sia limitata o inibita.

9. Il Direttore Area 9, responsabile dell'Ufficio CED provvede con propria determinazione a redigere l'elenco degli amministratori di sistema del Comune e a designarli individualmente con successivo atto precisandone le funzioni e specificandone l'ambito di attività.

   Gli estremi identificativi delle persone fisiche designate, con l'indicazione delle funzioni ad esse attribuite, è riportato in un elenco agli atti dell'Area stessa. Con cadenza annuale il Direttore d'Area 9, Responsabile dell'Ufficio CED verifica l'operato degli amministratori di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti. L'Area Sistemi Informativi adotta le misure necessarie a consentire un'attività di verifica dell'operato degli amministratori di sistema alla luce delle normative vigenti in merito al trattamento dei dati personali.

C) Il Trattamento dei dati senza l'ausilio di strumenti elettronici

Il trattamento "cartaceo" di dati personali deve essere garantito da particolari misure minime di sicurezza che debbono essere specificate dal Titolare del Trattamento dei dati nelle istruzioni impartite ai Responsabili ed agli incaricati per le diverse tipologie di trattamento, in particolare:

Il responsabile deve:

- coordinare tutte le operazioni di trattamento dei dati e vigilare sull'osservanza delle istruzioni impartite;
- curare l'informazione agli interessati relativa al trattamento dei dati e alla loro comunicazione;
- assegnare agli incaricati del trattamento le istruzioni per la corretta raccolta, elaborazione, consultazione e custodia dei dati;
- rettificare i dati su richiesta dell'interessato o d'ufficio, quando necessario;
- impartire le disposizioni operative per la sicurezza dell'accesso ai dati e ai documenti;
- curare l'eventuale relazione tra il trattamento effettuato e le singole banche dati gestite dall'Area Sistemi Informativi
- formulare proposte per l'eventuale distruzione, se consentito dalle norme, dei documenti contenenti dati non più necessari.

L'Incaricato deve:

- trattare i dati esclusivamente per gli scopi definiti dall'ambito di trattamento assegnato. I dati non possono in alcun modo essere comunicati a terzi non incaricati;

- osservare le norme di diligenza, prudenza e cautela per prevenire lo smarrimento, la distruzione o la perdita di documenti contenenti dati personali, e per prevenire l'accesso o il trattamento da parte di persone non autorizzate;
- assicurare la custodia delle chiavi di locali, armadi e cassettiere in cui sono conservati i documenti contenenti dati sensibili o giudiziari e, in caso di furto o smarrimento, fare pronta denuncia al responsabile;
- in caso di assenza dall'ufficio per cui il medesimo risulti non presidiato, proteggere in luogo custodito i singoli documenti temporaneamente estratti dall'archivio per motivi di lavoro e non lasciarli sulle scrivanie o alla libera visione di terzi;
- evitare di effettuare il trattamento dei dati personali in presenza di terzi che possano così venire a conoscenza, anche occasionalmente, dei dati.

1) QUADRO RIEPILOGATIVO DELLE MISURE MINIME PER I TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI E DEI RELATIVI CODICI

Codici di riferimento per la classificazione

Codice	Descrizione	Misure	Tipologia	Responsabili
5	Locali muniti di sicurezza	(chiusi a chiave in caso di assenza dell'incaricato)	organizzativa	incaricati
6	Archivi/contenitori muniti di sicurezza	(chiusi a chiave in caso di assenza dell'incaricato)	organizzativa	incaricati
7	Autorizzazione agli accessi fuori orario	organizzativa	Dirigente	PEG/ responsabile
8	Rilascio autorizzazione formale agli incaricati con le istruzioni per tutti gli operatori	organizzativa	Dirigente	PEG/ responsabile

Le Determinazioni di specificazione del presente documento dovranno fare riferimento nelle schede descrittive (allegato "B"), ai codici impiegati per la protezione dei dati, sopra evidenziati.
Qualora per un particolare trattamento i codici siano più di uno, vanno indicati tutti.

ALLEGATI:

"A1" Designazione responsabile esterno del trattamento dei dati.
"A2" Designazione dell'incaricato esterno del trattamento dei dati.
"B" Fac- simile scheda rilevazione Trattamento Dati Personali, Sensibili e Giudiziari da allegare alla determinazione dirigenziale.
"C" Convenzione per l'accesso in consultazione alle banche dati informatizzate del Comune di Selargius.

ALLEGATO ALLA DELIBERA
DI G. C. N 24 DEL 28/3/2012

IL SEGRETARIO COMUNALE
Dott.ssa M. Bonaria Pardu

ALLEGATO A1) - Designazione responsabile esterno del trattamento dei dati.

Comune di Selargius - Area..... .....

Oggetto: Nomina responsabile esterno del trattamento dei dati.

IL DIRETTORE D'AREA

Richiamati:
la disposizione del Sindaco del ..... protocollo n°. ..... , con la quale il sottoscritto è stato nominato responsabile delle banche dati e del trattamento dei dati personali dell'Area .....;
l'art.29 del D Lgs n° 196/2003 "Codice in materia di protezione dei dati personali", relativo al Responsabile del trattamento;
il Regolamento per il trattamento e la tutela dei dati personali, approvato con deliberazione del Consiglio Comunale n° 90 del 10/11/2011;
il Regolamento per il trattamento dei dati sensibili e giudiziari approvato con deliberazione del Consiglio Comunale n° 13 del 31/01/2006;
il Disciplinare Tecnico in materia di misure minime di sicurezza approvato con la deliberazione della Giunta Comunale n° ____ del __/__/____;
il contratto/convenzione/concessione stipulato in data .....;
la comunicazione effettuata da .....in data ..... recante la designazione di ...., quale soggetto idoneo a ricoprire il ruolo di responsabile del trattamento;
Considerato che in capo al soggetto individuato e designato sussistono i requisiti di esperienza, capacità e affidabilità di cui all'art. 29, comma 2, del decreto legislativo 30 giugno 2003, n° 196;
Visto il D. Lgs. n° 267/2000;

Designa

_____ con sede in _____ nella persona di----------
-

----------, Responsabile del trattamento dei dati personali effettuato nello svolgimento di operazioni strettamente necessarie e strumentali rispetto all'esecuzione del contratto/ convenzione/concessione.

In tale qualità, _____ è tenuto al rispetto delle disposizioni di legge e di regolamento in materia di tutela dei dati personali.
In particolare:

- osservare il decreto legislativo 30 giugno 2003, n° 196 e le altre disposizioni legislative e regolamentari in materia di riservatezza delle persone, osservando i principi di liceità e correttezza;
- censire i trattamenti di dati personali e le banche dati gestite per conto dell'amministrazione;
- nominare gli incaricati del trattamento sulla base dello schema di incarico fornito dal Comune (Allegato A2) nonché impartire loro le istruzioni necessarie per un corretto, lecito, sicuro trattamento dei dati e per la loro custodia;
- tenere un elenco aggiornato degli incaricati del trattamento che dovrà essere fornito, a richiesta, al Comune ;
- coordinare tutte le operazioni di trattamento dei dati e vigilare sull'osservanza delle istruzioni impartite;
- attuare gli obblighi di informativa nei confronti degli interessati;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del D. Lgs. 30 giugno 2003, n° 196, riferendo in ogni caso all'ufficio _____;
- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre e aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni agli articoli da 31 a 36 e allegato B del D. Lgs. 30 giugno 2003 n° 196 e da ogni altra disposizione in materia, nonché adeguare il sistema alle future norme regolamentari in materia di sicurezza;
- elaborare una relazione trimestrale sullo stato degli adempimenti previsti dal D. Lgs. 30 giugno 2003 n° 196.

Nel caso in cui l'oggetto del contratto o della convenzione comporti l'utilizzazione di applicazioni o banche dati del Comune, per ottenere le relative autorizzazioni all'accesso il responsabile esterno dovrà fornire al Direttore d'Area all'inizio della collaborazione, l'elenco degli incaricati al trattamento dei dati per i quali si richiede il rilascio delle credenziali.
Le credenziali che abilitano gli incaricati alle applicazioni e alle banche dati hanno una durata massima di dodici mesi, trascorsi i quali esse verranno automaticamente disabilitate.
Pertanto, qualora il contratto/convenzione/concessione abbia una durata superiore all'anno, il responsabile esterno del trattamento dei dati, al fine di evitare che le credenziali degli incaricati siano automaticamente disabilitate alla scadenza dei dodici mesi, dovrà fornire all'amministrazione, due mesi prima della scadenza delle stesse, l'elenco aggiornato degli incaricati che sostituirà quello precedentemente fornito.

Qualsiasi utilizzo e trattamento del dato improprio o non conforme al D. Lgs. 30 giugno 2003 n° 196 comporterà l'esclusiva e piena responsabilità della società / ente ....., rimanendo il Comune escluso da ogni responsabilità al riguardo

Data
Il Direttore d'Area

Per accettazione (data, qualifica e firma) .....

ALLEGATO ALLA DELIBERA
DI G.C. N. 24 DEL 28/3/2012

Allegato A2 - Nomina dell'incaricato esterno del trattamento dei dati.

Oggetto: Nomina dell'incaricato esterno del trattamento di dati.

La Società /Ente..... nella persona di .....
Premesso che, con atto PG ..... del ....., è stato designato responsabile del trattamento dei dati per lo svolgimento delle operazioni strettamente necessarie e strumentali rispetto all'esecuzione del contratto/convenzione/concessione stipulato con il Comune di Selargius in data ..... ;
Richiamato l'art. 30 del D. Lgs. n° 196/2003 "Codice in materia di protezione dei dati personali", relativo agli Incaricati del trattamento;

INCARICA

il Sig.....delle seguenti operazioni di trattamento :
.....
.....

A tal fine impartisce le seguenti istruzioni :

- I dati possono essere trattati esclusivamente per gli scopi definiti dall'ambito del trattamento indicato e non possono in alcun modo essere comunicati a terzi non incaricati.
- Concluso l'incarico assegnato, non potrà conservare copia dei dati e dei programmi del Comune di Selargius né alcuna documentazione ad essi inerente.
- Devono essere osservate le norme di diligenza, prudenza e cautela finalizzate a prevenire ed evitare lo smarrimento, la distruzione o la perdita di documenti contenenti dati personali, nonché l'accesso o il trattamento da parte di persone non autorizzate.
- A tale fine deve essere assicurata la custodia e l'uso esclusivo e personale dei dispositivi di autenticazione rilasciati per il trattamento con l'ausilio di strumenti elettronici, e non deve essere lasciato incustodito e accessibile lo strumento elettronico durante la sessione di trattamento, anche in caso di assenza temporanea dall'ufficio (es. pausa caffè) e in particolare negli orari di accesso agli uffici da parte del pubblico esterno.
- Analogamente deve essere assicurata la custodia delle chiavi di locali, armadi e cassettiere in cui sono conservati i documenti contenenti dati personali e, in caso di furto o smarrimento, deve essere fatta pronta denuncia al responsabile.

- In caso di assenza dall'ufficio per cui il medesimo risulti non presidiato, i singoli documenti temporaneamente estratti dall'archivio per motivi di lavoro devono essere protetti in luogo custodito e non possono essere lasciati sulle scrivanie o alla libera visione di terzi.
- Nel corso del trattamento devono essere assunte adeguate misure e adottati appositi accorgimenti affinché i dati trattati non vengono portati alla conoscenza anche occasionale di soggetti terzi che si trovino nei luoghi in cui il trattamento è effettuato.

Data _____

Il Responsabile .....

Per ricevuta .....

ALLEGATO ALLA DELIBERA
DI G. C. N. 24 DEL 28/3/2017

ALLEGATO B) - Fac- simile scheda rilevazione Trattamento Dati Personali, Sensibili e Giudiziari da allegare alla determinazione dirigenziale

Tipologia di trattamento - Tipologia dati

Mappa dei trattamenti effettuati per aree:

Nella seguente tabella si riassumono i trattamenti effettuati in relazione alle unità organizzative:

- sull'asse verticale si riportano i dati personali oggetto di trattamento
- sull'asse orizzontale si riportano le unità organizzative in cui si suddivide l'organizzazione.

L'apposizione del simbolo **X**, in corrispondenza della casella di intersezione tra le due coordinate, significa che una determinata unità organizzativa procede al trattamento dei dati indicati nelle righe:

TIPI DI DATI TRATTATI

1 - Dati comuni relativi a clienti/utenti/dipendenti	X	X	X	X	X	X	X	X	X	X
2 - Dati comuni relativi a fornitori	X	X	X	X	X	X	X	X	X	X
3 - Dati comuni relativi ad altri soggetti	X	X	X	X	X	X	X	X	X	X
4 - Dati biometrici relativi a clienti / personale /										X
5 - Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone / oggetti									X	X
6 - Dati relativi allo svolgimento di attività economiche e alle informazioni commerciali	X	X	X		X	X	X	X	X	X
7 - Dati di natura giudiziaria relativi a	X	X	X	X	X	X	X	X	X	X
8 - Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile	X			X						X
9 - Dati di natura anche sensibile relativi a clienti / utenti / membri / pazienti.....	X	X	X	X					X	X
10 Dati idonei a rivelare lo stato di salute e/o la vita sessuale di pazienti / degenti.....		X								X
11 - Dati idonei a rivelare l'affezione da virus HIV		X								X
12 - Dati di natura genetica										
	A	B	C	D	E	F	G	H	I	J

La legenda delle unità organizzative è la seguente:

A. Sindaco, Segretario Generale
B. Area 1 Area Politiche Sociali, Pubblica Istruzione, Promozione Culturale e Sportiva
C. Area 2 Area Finanziaria, Contabile e del Patrimonio
D. Area 3 Area Tributi Locali, Attività Produttive e Commerciali, Economato
E. Area 4 Area Amministrazione e Gestione Risorse Umane, Servizi Demografici
F. Area 5 Area Programmazione Pianificazione, Tutela e Controllo del Territorio
G. Area 6 Area Progettazione e Appalti Opere Pubbliche

H. Area 7 Area Servizi Ambientali e Tecnologici, Manutenzione Patrimonio Immobiliare Comunale, Protezione Civile
I. Area 8 Area Polizia Locale, Ordine Pubblico e Sicurezza, Controllo del territorio
J. Area 9 Area Segreteria Generale, Affari Generali, Contratti, Biblioteca, Musei e Archivio, Servizi Informatici

Mappa dei trattamenti per aree in relazione agli strumenti utilizzati per il trattamento:

- sull'asse verticale si riportano i dati oggetto di trattamento.
- sull'asse orizzontale si riportano gli uffici (codificati come da legenda nella pagina successiva) in cui è suddivisa la sede.

I valori inseriti all'interno di ogni singola cella evidenziano la relazione dato/ufficio/strumento utilizzato per il trattamento.

TIPI DI DATI TRATTATI

1 - Dati comuni relativi a clienti	G1 K1	C6 G13 K13	C4 G9 K9	C6 G12 K12	C6 G14 F5 K14	C6 G16 K16	C5 G10 K11	C5 G14 K14	K10 C6 G10 F2	C10 G18 K46
2 - Dati comuni relativi a fornitori	G1 K1	C6 G13 K13	C4 G9 K9	C6 G12 K12	C6 G14 F5 K14	C6 G16 K16	C5 G10 K11	C5 G14 K14	K10 C6 G10 F2	C10 G18 K46
3 - Dati comuni relativi ad altri soggetti	G1 K1	C6 G13 K13	C4 G9 K9	C6 G12 K12	C6 G14 F5 K14	C6 G16 K16	C5 G10 K11	C5 G14 K14	K10 C6 G10 F2	C10 G18 K46
4 - Dati biometrici relativi a clienti / personale										C10 G18 K46
5 - Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone / oggetti									K10 C6 G10 F2	
6 - Dati relativi allo svolgimento di attività economiche e a informazioni commerciali	G1 K1	C6 G13 K13	C4 G9 K9		C6 G14 F5 K14	C6 G16 K16	C5 G10 K11	C5 G14 K14	K10 C6 G10 F2	C10 G18 K46
7 - Dati di natura giudiziaria relativi a	G1 K1	C6 G13 K13	C4 G9 K9	C6 G12 K12	C6 G14 F5 K14	C6 G16 K16	C5 G10 K11	C5 G14 K14	K10 C6 G10 F2	C10 G18 K46
8 - Dati relativi al personale, nonché a candidati per diventarlo, anche sensibili	G1 K1			C6 G12 K12						C10 G18 K46
9 - Dati di natura anche sensibile relativi a clienti / utenti / membri /	G1 K1	C6 G13 K13	C4 G9 K9	C6 G12 K12					K10 C6 G10 F2	C10 G18 K46
10 Dati idonei a rivelare lo stato di salute e/o la vita sessuale di pazienti / degenti.....		C6 G13 K13								C10 G18 K46
11 - Dati idonei a rivelare l'affezione da virus HIV		C6 G13 K13								
12 - Dati di natura genetica										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

Legenda degli strumenti utilizzati per il trattamento:

A. Armadi blindati
B. Armadi ignifughi
C. Armadi con chiusura a chiave
D. Armadi senza chiusura a chiave
E. Schedari
F. Scaffalature
G. Cassettiera con chiusura a chiave
H. Cassettiera senza chiusura a chiave
I. Computer stand alone
J. Computer in rete privata
K. Computer in rete pubblica
L. PC Portatile
M. Classificatori cassetti con serratura
N. Stampanti
O. Cassaforte
P. Fotocopiatrice
Q. Impianto registrazione immagini

Codice uffici:

1. Sindaco, Segretario Generale
2. Area Politiche Sociali, Pubblica Istruzione, Promozione Culturale e Sportiva
3. Area Finanziaria, Contabile e del Patrimonio
4. Area Tributi Locali, Attività Produttive e Commerciali, Economato
5. Area Amministrazione e Gestione Risorse Umane, Servizi Demografici
6. Area Programmazione Pianificazione, Tutela e Controllo del Territorio
7. Area Progettazione e Appalti Opere Pubbliche
8. Area Servizi Ambientali e Tecnologici, Manutenzione Patrimonio Immobiliare Comunale, Protezione Civile
9. Area Polizia Locale, Ordine Pubblico e Sicurezza, Controllo del territorio
10. Area Segreteria Generale, Affari Generali, Contratti, Biblioteca, Musei e Archivio, Servizi Informatici

ALLEGATO ALLA DELIBERA DI G.C. N. 24 DEL 28/3/2012

ALLEGATO C – SCHEMA DI CONVENZIONE

CONVENZIONE TRA IL COMUNE DI SELARGIUS E ..... PER L'ACCESSO TELEMATICO ALLA BANCA DATI .....

Il Comune di Selargius, in seguito denominato Comune, con sede in ..... cod. fiscale ..... rappresentato da ..... nella qualità di Direttore d'Area ..... e titolare del trattamento della banca dati .....

e

....., in seguito denominato Ente , con sede in ..... cod. fiscale ..... rappresentato da ..... nella propria qualità di .....

Vista la nota del ..... pervenuta al protocollo generale in data ..... n..... con la quale il predetto Ente ha chiesto di aderire alla convenzione che consente l'accesso alla banca dati .....essenziale per lo svolgimento dei propri compiti istituzionali, specificando gli adempimenti normativi, le finalità istituzionali perseguite e i motivi che titolano l'Ente all'accesso dei dati;

Valutata la legittimità della richiesta in considerazione delle motivazioni di pubblica utilità rappresentate;

Vista la propria determinazione n. ..... del ..... con la quale si è ritenuto di addivenire alla stipula della convenzione;

Richiamata la delibera della Giunta Comunale n..... del ..... con cui è stato definito lo schema di convenzione per l'accesso alle banche dati

Visti *(nella convenzione andranno inserite le leggi di riferimento):*

- .....
- .....
- .....
- l'art. 43 del D.P.R.28/12/2000, n° 445;
- il D. Lgs 30/03/2003, n° 196 (Codice della privacy);
- il D. Lgs 07/03/2005, n° 82 (Codice dell'Amministrazione Digitale)

Convengono quanto segue

Art.1 Oggetto della convenzione

Il Comune autorizza l'accesso alla banca dati informatizzata degli archivi ..... per le specifiche finalità istituzionali secondo le modalità e nei limiti specificati nei successivi articoli.

L'Ente si impegna a non richiedere al Comune controlli sulle autocertificazioni rese dai cittadini o comunque informazioni su dati che possono essere assunti attraverso l'accesso alla banca dati .....

L'accesso a dati ulteriori rispetto a quelli ai quali viene consentito l'accesso con la presente convenzione potrà essere autorizzato solo se l'Ente motiverà la propria richiesta sulla base di specifiche finalità e competenze istituzionali dichiarando, nel contempo la pertinenza e necessità dei dati richiesti.

Art.2 – Utilizzo dei dati

L'Ente si impegna a:

- utilizzare le informazioni acquisite dal titolare esclusivamente per le finalità dichiarate, nel rispetto della normativa vigente, anche in materia di consultazione delle banche dati, osservando le misure di sicurezza ed i vincoli di riservatezza previsti dal Codice della Privacy;
- procedere al trattamento dei dati personali, in particolare di quelli sensibili, osservando le misure di sicurezza ed i vincoli di riservatezza previsti dal Codice della Privacy rispettando i canoni di pertinenza e non eccedenza nel trattamento delle informazioni acquisite;

- garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, né in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, provvedendo ad impartire, ai sensi dell'art. 30 del Codice della Privacy, precise e dettagliate istruzioni agli incaricati del trattamento, richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati;
- non duplicare i dati resi disponibili e non creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato l'accesso;
- garantire che l'accesso ai dati verrà consentito esclusivamente a personale o assimilati ovvero a soggetti che siano stati designati dal fruitore quali incaricati o responsabili esterni del trattamento dei dati;
- cancellare i dati ricevuti dal titolare non appena siano state utilizzate le informazioni secondo le finalità dichiarate;
- formare gli utenti abilitati sulle specifiche caratteristiche, proprietà e limiti del sistema utilizzato per l'accesso ai dati e controllarne il corretto utilizzo.
- garantire l'adozione al proprio interno delle regole di sicurezza atte ad adottare procedure di registrazione che prevedano il riconoscimento diretto e l'identificazione certa dell'utente e adottare regole di gestione delle credenziali di autenticazione e modalità che ne assicurino adeguati livelli di sicurezza . Nel caso le credenziali siano costituite da una coppia username/password, devono essere previste politiche di gestione della password che rispettino le misure minime di sicurezza previste dal Codice della Privacy e la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza adeguata.
- utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalità con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti"robot") allo scopo di velocizzare le attività e creare autonome banche dati non conformi alle finalità per le quali è stato autorizzato all'accesso;
- comunicare tempestivamente all'amministrazione titolare:
    - eventuali incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza;
    - ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;
    - ogni modificazione tecnica e/o organizzativa del proprio dominio, che comporti l'impossibilità di garantire l'applicazione delle regole di sopra riportate e/o la loro perdita di efficacia
    - ogni innovazione normativa/ organizzativa che comporti una revisione della presente convenzione. In tal caso il Comune si riserva di modificare la convenzione e le modalità di accesso ai dati sulla base delle innovazioni normativa e/o organizzative intervenute
- garantire, in caso di cooperazione applicativa, che i servizi resi disponibili verranno esclusivamente integrati con il proprio sistema informativo e non saranno resi disponibili a terzi né direttamente né indirettamente per via informatica.

L'Ente dichiara di essere consapevole della possibilità di controlli da parte del Comune previsti dal Codice della privacy per verificare il rispetto dei vincoli di utilizzo dei servizi.
Per l'espletamento di tali controlli, che potranno essere effettuati anche presso le sedi del fruitore dove viene utilizzato il servizio,
l'Ente si impegna a fornire ogni necessaria collaborazione

Art. 3 – Modalità di accesso e servizi erogati

Il Comune consente l'accesso telematico tramite la cooperazione applicativa/la rete internet/il trasferimento di dati attraverso file/la posta elettronica certificata *(nella convenzione dovranno essere indicate le possibili opzioni tra le modalità di accesso sopra indicate o altre eventualmente individuate)* ai servizi di ricerca/consultazione/scaricamento

dei dati/ altro *(nella convenzione dovranno essere individuate le possibili opzioni tra quelle indicate o altre eventualmente individuate).*
La descrizione dell'infrastruttura tecnologica resa disponibile per l'accesso ai dati, le modalità di fruizione dei dati e le regole di accesso, i livelli di servizio forniti, le regole minime di sicurezza sono contenute **nell'Allegato 1** che costituisce parte integrante della presente convenzione.

Art. 4 – Titolarità della banca dati
Il Comune conserva la piena ed esclusiva proprietà delle informazioni contenute nella banca dati ..... e del sistema di ricerca; ha l'esclusiva competenza di gestire, definire e modificare i sistemi di elaborazione, ricerca, rappresentazione e organizzazione dei dati; ha altresì la facoltà di variare la base informativa in relazione alle proprie esigenze istituzionali, organizzative e tecnologiche.
La banca dati è di esclusiva titolarità del Comune.
Qualora intervengano modificazione delle circostanze di fatto e di diritto, l'Ente ha la facoltà di recedere dalla presente convenzione, previo preavviso di almeno trenta giorni da inviare al Comune con raccomandata con ricevuta di ritorno o strumento equivalente (posta elettronica certificata).

Art. 5 – Responsabile del trattamento
L'Ente individua come responsabile del trattamento ....., alla cui nomina si provvederà, ai sensi dell'articolo 29 del D. Lgs n° 196/2003, con specifico atto di cui **all'Allegato 2**, nel rispetto delle prescrizioni e delle modalità di cui al Disciplinare Tecnico in materia di misure di sicurezza adottato dal Comune di Selargius, che l'Ente dichiara di ben conoscere e che si impegna a rispettare.
Il responsabile del trattamento si impegna a nominare gli incaricati del trattamento sulla base dello schema di incarico di cui **all'Allegato 3**.
In caso di sostituzione del responsabile, l'Ente si impegna a comunicare tempestivamente il nominativo del nuovo responsabile al Comune che provvederà alla nomina dello stesso.

Art. 6 – Limitazione e responsabilità
Il Comune è sollevato da ogni responsabilità contrattuale ed extracontrattuale per danni diretti o indiretti che possano derivare in conseguenza dell'uso dei dati attinti dalla banca dati ..... del Comune nonché per i danni derivanti da interruzioni, ritardi o errori nella elaborazione e/o trasmissione dei dati, ovunque si verifichino, in qualunque forma si manifestino e da qualsiasi causa siano determinati.
L'Ente si impegna ad utilizzare le informazioni ottenute tramite il collegamento esclusivamente per fini istituzionali, nel rispetto della normativa vigente, dei principi di necessità, pertinenza e non eccedenza e del diritto alla riservatezza e si assume ogni responsabilità in ordine all'utilizzo e al trattamento improprio o illecito e alle conseguenti eventuali richieste di risarcimento da parte di terzi, sollevando al riguardo il Comune da ogni responsabilità.

Art.7- Costi
La convenzione non ha oneri economici salvo che per elaborazioni aggiuntive. Rimangono a carico dell'Ente i costi derivanti dalla connessione a Internet *(da inserire in convenzione se l'accesso avviene attraverso internet)* e i costi derivanti dalla realizzazione dell'infrastruttura di collegamento con il Comune (connessione a Internet o altro).

Art.8 - Durata
La presente convenzione avrà durata di ..... anni dalla data di sottoscrizione con possibilità di rinnovo esplicito per altri ..... anni.
Il Comune si riserva la possibilità di recedere in qualsiasi momento dalla presente convenzione a suo insindacabile giudizio, previa comunicazione inviata con raccomandata

con ricevuta di ritorno o altro strumento analogo, con un preavviso di 15 giorni lavorativi qualora non siano rispettate le condizioni in essa previste o nel caso del verificarsi di eventi che motivino la cessazione della comunicazione dei dati (interventi normativi, ecc.).

Art.9 – Foro competente
Per tutte le controversie direttamente o indirettamente connesse alla presente convenzione è competente il Foro di Cagliari

.

Art.10 - Registrazione
La presente convenzione, redatta in due originali, non è soggetta a registrazione ai sensi dell'art.1 della tabella allegata al DPR 26.4.1986 n.131 ed è esente da imposta di bollo ai sensi dell'art.16 – Tabella allegato B – del DPR 642/72.

Art. 11 – Spese contrattuali
Non sono previste spese contrattuali.

Art. 12 - Informativa
Le parti dichiarano di essersi scambiati la reciproca informativa ai sensi dell'art. 13 del D. Lgs. n° 196/2003

Selargius, ...

Per l'Ente ***Per il Comune***

ALLEGATO 1- CRITERI TECNICI PER LE MODALITÀ DI ACCESSO AI DATI

Glossario

Accesso telematico: la possibilità che soggetti esterni all'amministrazione titolare accedano a specifici dati attraverso una rete telematica.

Comune: l'Amministrazione titolare della banca dati che mette a disposizione i relativi servizi di accesso sulla base della convenzione predisposta in ottemperanza a quanto previsto dall'art.58 comma 2 del Codice dell'Amministrazione Digitale.

Ente: l'amministrazione che accede ai dati resi disponibili dal Comune, secondo le regole e con le modalità definite nella convenzione a cui l'ente aderisce.

Banca dati: l'insieme di dati omogenei, memorizzati in uno o più archivi informatici, organizzati e resi accessibili mediante uno strumento software.

Cooperazione applicativa: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'interazione dei metadati, delle informazioni e dei procedimenti amministrativi.

Posta elettronica certificata: il sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili.

Disponibilità dei dati: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge.

Ricerca dei dati: la possibilità di individuare l'esistenza di dati in base al contenuto di metadati corrispondenti.

Consultazione dei dati: la possibilità di accedere ai dati in sola visualizzazione e lettura senza che sussista un sistema tecnologico che ne consenta l'estrazione. Il dato rimane, pertanto, all'interno del sistema informativo proprietario.

Scaricamento (fruibilità) dei dati: la possibilità di trasferire i dati nei sistemi informativi automatizzati di un'altra amministrazione o ente. Il trasferimento del dato non ne modifica la titolarità. *(Inserire nella convenzione l'eventuale elencazione e definizione dei documenti informatici a cui si accede)*

Descrizione dell'infrastruttura tecnologica resa disponibile per l'accesso ai dati: L'accesso ai dati è reso disponibile attraverso il Sistema pubblico di connettività/altra infrastruttura (*A seconda della tipologia di dati a cui si chiede l'accesso va indicata l'infrastruttura tecnologica utilizzata)*

Modalità di accesso telematico e regole di accesso.

L'accesso telematico alla banca dati informatizzata degli archivi ..... è consentita tramite la cooperazione applicativa/la rete internet/il trasferimento di dati attraverso file/la posta elettronica certificata. *(A seconda della tipologia di dati vanno indicate le possibili opzioni tra le modalità di accesso sopra indicate o altre eventualmente individuate. La scelta della modalità del trasferimento attraverso file deve essere adeguatamente motivata).*

L'Ente si impegna a comunicare al Comune l'elenco degli utenti che devono essere abilitati all'interrogazione della banca dati, allegando una scheda identificativa nella quale devono essere indicate le seguenti informazioni: nome e cognome; codice fiscale; numero di telefono e sede di lavoro

L'Ente si impegna ad incaricare del trattamento ogni operatore indicato in elenco utilizzando **l'Allegato 3** e a responsabilizzarlo in ordine al corretto utilizzo dei dati, alle problematiche inerenti alla sicurezza e a quanto stabilito dalla presente convenzione.

Alla banca dati potranno accedere esclusivamente gli incaricati dotati delle proprie credenziali d'accesso.

Al fine di consentire lo svolgimento dell'attività di accesso alla banca dati, il Comune si impegna a fornire in busta chiusa ad ognuno dei suddetti operatori le credenziali di autenticazione individuali (userid e password provvisoria).

Al primo accesso al sistema informatico, gli incaricati del trattamento dei dati dovranno sostituire la password provvisoria loro assegnata con una di loro scelta.
Le credenziali di autenticazione hanno una durata massima di 12 mesi. Al fine di evitare che le credenziali degli operatori incaricati siano automaticamente disabilitate allo scadere dei 12 mesi, il responsabile del trattamento dei dati è tenuto, due mesi prima della scadenza delle stesse, a comunicare per iscritto al Comune l'elenco aggiornato degli incaricati in sostituzione di quello precedentemente fornito, dando altresì conferma del permanere delle finalità e delle motivazioni per cui è stato concesso l'accesso alla banca dati .
In caso di cessazione di un operatore dall'incarico, l' Ente si impegna a darne tempestiva notizia al Comune tramite l'indirizzo e.mail ..... affinché venga disabilitato.

Regole minime di sicurezza
L'Ente si impegna a dare disposizioni ai propri utenti affinché la password sia mantenuta segreta, venga conservata adeguatamente e non venga né comunicata né divulgata.
La password dovrà essere modificata alle scadenze temporali indicate nel Disciplinare Tecnico delle misure minime di sicurezza del Comune di Selargius.
Il collegamento è consentito agli operatori incaricati esclusivamente durante lo svolgimento della propria attività lavorativa.
Le stazioni di lavoro collegate con la banca dati comunale dovranno essere collocate in luogo non accessibile al pubblico e poste sotto la responsabilità dell'operatore designato.
Al fine di consentire agli operatori l'accesso alle sole informazioni pertinenti e non eccedenti rispetto al proprio profilo e alla finalità istituzionale perseguita dalla convenzione stessa, l'accesso ai dati sarà consentito attraverso la segmentazione degli stessi *(frase da inserire nell'allegato qualora si reputi necessaria la profilazione degli accessi)*
Il Comune è legittimato a registrare tutti gli accessi sul proprio sistema informativo memorizzando le posizioni interrogate in appositi files, al fine di prevenire o correggere malfunzionamenti del sistema e garantire l'efficienza dello stesso, di mettere i file a disposizione dell'autorità giudiziaria, qualora vengano richiesti, nonché di effettuare periodici controlli che verranno eseguiti con le seguenti modalità: .....
La registrazione degli accessi verrà conservata per un periodo di tempo di .....
L'Ente dichiara che le modalità con cui verranno trattati i dati durante il loro ciclo di vita sono le seguenti: .....
L'Ente garantisce l'adeguatezza del proprio standard di sicurezza della protezione dei dati e l'adozione di ogni misura necessaria ad evitare indebiti utilizzi dei dati stessi, dichiarandosi fin d'ora disponibile a seguire anche le indicazioni tecniche fornite dal Comune.
Periodici controlli potranno essere effettuati dal Garante della privacy, con l'eventuale supporto del Comune, in merito all'uso dei dati da parte dell'Ente.

Servizi forniti
I servizi erogati sono i seguenti: ricerca/consultazione/scaricamento/altro *(indicare i servizi forniti sulla base di quanto concordato con l'Ente)*
Qualora l'Ente abbia necessità di disporre di elenchi di dati si procederà con le seguenti modalità:.....

Livelli di servizio
Il servizio avverrà con le seguenti modalità: .....
In caso di interruzioni programmate il Comune informerà attraverso la posta elettronica gli operatori interessati dei tempi previsti di interruzione e del ripristino del servizio.
Gli orari in cui il servizio di assistenza è operativo sono i seguenti: ..... In caso di malfunzionamento nell'accesso dei dati l'Ente potrà rivolgersi a .....

Periodicità dell'aggiornamento dei dati
I dati oggetto di accesso sono aggiornati ogni.....

Allegato 2 - Designazione del responsabile esterno del trattamento

Comune di Selargius - Area..... .....

Oggetto: Nomina responsabile del trattamento di dati personali

IL DIRRETTORE D'AREA

Richiamati: ·
- la disposizione del Sindaco del ..... protocollo n°. ..... , con la quale il sottoscritto è stato nominato responsabile delle banche dati e del trattamento dei dati personali dell'Area .....;
- l'art.29 del D Lgs n° 196/2003 "Codice in materia di protezione dei dati personali", relativo al Responsabile del trattamento;
- il Regolamento per il trattamento e la tutela dei dati personali, approvato con deliberazione del Consiglio Comunale n° 90 del 10/11/2011;
- il Regolamento per il trattamento dei dati sensibili e giudiziari approvato con deliberazione del Consiglio Comunale n° 13 del 31/01/2006;
- il Disciplinare Tecnico in materia di misure minime di sicurezza approvato con deliberazione della Giunta Comunale n° ____ del __/__/____;
- la convenzione per l'accesso alla banca dati ..... del Comune stipulata in data .....;
- la comunicazione effettuata da .....in data ..... recante la designazione di ...., quale soggetto idoneo a ricoprire il ruolo di responsabile del trattamento;

Considerato che in capo al soggetto individuato e designato sussistono i requisiti di esperienza, capacità e affidabilità di cui all'art. 29, comma 2, del decreto legislativo 30 giugno 2003, n° 196;
Visto il D. Lgs. n° 267/2000;

NOMINA

_____ con sede in _____ nella persona di ----------

Responsabile del trattamento dei dati personali effettuato nello svolgimento di operazioni strettamente necessarie e strumentali rispetto all'esecuzione della convenzione suddetta.
In tale qualità, _____ è tenuto al rispetto delle disposizioni di legge e di regolamento in materia di tutela dei dati personali.
In particolare:
- osservare il D. Lgs. 30 giugno 2003, n° 196 e le altre disposizioni legislative e regolamentari in materia di riservatezza delle persone osservando i principi di liceità e correttezza;

- nominare gli incaricati del trattamento sulla base dello schema di incarico fornito dal Comune nonché impartire loro le istruzioni necessarie per un corretto, lecito, sicuro trattamento dei dati e per la loro custodia;
- tenere un elenco aggiornato degli incaricati del trattamento che dovrà essere fornito, a richiesta, al Comune ;
- coordinare tutte le operazioni di trattamento dei dati e vigilare sull'osservanza delle istruzioni impartite;
- attuare gli obblighi di informativa nei confronti degli interessati;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo 30 giugno 2003 n. 196, riferendo in ogni caso all'ufficio _____;
- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre e aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni agli articoli da 31 a 36 e allegato B del decreto legislativo 30 giugno 2003 n. 196 e da ogni altra disposizione in materia, nonché adeguare il sistema alle future norme regolamentari in materia di sicurezza;
- elaborare una relazione trimestrale sullo stato degli adempimenti previsti dal decreto legislativo 30 giugno 2003 n. 196.

Il responsabile esterno dovrà fornire al Direttore d'Area all'inizio della collaborazione, l'elenco degli incaricati al trattamento dei dati per i quali si richiede il rilascio delle credenziali.

Le credenziali che abilitano gli incaricati all'utilizzazione delle applicazioni e delle banche dati hanno una durata massima di dodici mesi, trascorsi i quali esse verranno automaticamente disabilitate.

Il responsabile esterno del trattamento dei dati, al fine di evitare che le credenziali degli incaricati siano automaticamente disabilitate alla scadenza dei dodici mesi, dovrà fornire all'amministrazione, due mesi prima della scadenza delle stesse, l'elenco aggiornato degli incaricati che sostituirà quello precedentemente fornito.

Qualsiasi utilizzo e trattamento del dato improprio o non conforme al D. Lgs. N° 196/2003 comporterà l'esclusiva e piena responsabilità della società/ente ....., rimanendo il Comune escluso da ogni responsabilità al riguardo.

Data .....

Il Direttore d'Area _____

Per accettazione (data, qualifica e firma) .....

Allegato 3 Designazione dell'incaricato esterno del trattamento dei dati.

Oggetto: Nomina dell'incaricato esterno del trattamento di dati.

La Società /Ente..... nella persona di .....
Premesso che, con atto PG ..... del ....., è stato designato responsabile del trattamento dei dati personali per lo svolgimento delle operazioni strettamente necessarie e strumentali rispetto all'esecuzione della convenzione stipulata con il Comune di Selargius in data ..... per l'accesso alla banca dati .....;
Richiamato l'art. 30 del D. Lgs. n° 196/2003 "Codice in materia di protezione dei dati personali", relativo agli Incaricati del trattamento;

INCARICA

il Sig.....delle seguenti operazioni di trattamento :
.....
.....

A tal fine impartisce le seguenti istruzioni :

- I dati possono essere trattati esclusivamente per gli scopi definiti dall'ambito del trattamento indicato e non possono in alcun modo essere comunicati a terzi non incaricati.
- Concluso l'incarico assegnato, non potrà conservare copia dei dati e dei programmi del Comune di Selargius né alcuna documentazione ad essi inerente.
- Devono essere osservate le norme di diligenza, prudenza e cautela finalizzate a prevenire ed evitare lo smarrimento, la distruzione o la perdita di documenti contenenti dati personali, nonché l'accesso o il trattamento da parte di persone non autorizzate.
- A tale fine deve essere assicurata la custodia e l'uso esclusivo e personale dei dispositivi di autenticazione rilasciati per il trattamento con l'ausilio di strumenti elettronici, e non deve essere lasciato incustodito e accessibile lo strumento elettronico durante la sessione di trattamento, anche in caso di assenza temporanea dall'ufficio (es. pausa caffè) e in particolare negli orari di accesso agli uffici da parte del pubblico esterno.
- Analogamente deve essere assicurata la custodia delle chiavi di locali, armadi e cassettiere in cui sono conservati i documenti contenenti dati personali e, in caso di furto o smarrimento, deve essere fatta pronta denuncia al responsabile.
- In caso di assenza dall'ufficio per cui il medesimo risulti non presidiato, i singoli documenti temporaneamente estratti dall'archivio per motivi di lavoro devono essere protetti in luogo custodito e non possono essere lasciati sulle scrivanie o alla libera visione 42 di terzi.

- Nel corso del trattamento devono essere assunte adeguate misure e adottati appositi accorgimenti affinché i dati trattati non vengono portati alla conoscenza anche occasionale di soggetti terzi che si trovino nei luoghi in cui il trattamento è effettuato.

Data _____

Il Responsabile .....

Per ricevuta .....