DOCUMENTO SULLA SICUREZZA DEI DATI PERSONALI

(approvato con deliberazione della Giunta Comunale n. 748 del 18/12/2018)

INDICE

PARTE I - DISPOSIZIONI GENERALI

1. Finalità

1. Il Comune di Modena effettua i trattamenti dei dati personali nel rispetto delle disposizioni normative e regolamentari in materia di protezione delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, attenendosi a principi di liceità, correttezza, trasparenza, riservatezza, nel rispetto delle Misure Minime di sicurezza ICT adottate con determinazione del Dirigente del Servizio Progetti Telematici, Comunicazione e Città intelligente n. 2908/2017 e successive modifiche e integrazioni;

2. In ossequio all'art.5 del Regolamento UE 2016/679 (d'ora in avanti RGPD), i dati personali oggetto di trattamento sono:

a) trattati in modo lecito, corretto e trasparente;

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);

d) esatti e, se necessario, aggiornati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore al conseguimento delle finalità per cui sono trattati, al termine del quale potranno essere conservati, con le modalità e nel rispetto delle disposizioni normative in materia, nel caso di ulteriori obblighi di conservazione previsti da disposizioni di legge o per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

f) trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti, o dalla perdita, dalla distruzione o da danni accidentali.

2. Oggetto

1. Il presente Documento ha per oggetto le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio con riferimento ad ogni trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

3. Titolarità del trattamento dei dati personali

1. Il Comune di Modena, rappresentato, ai fini previsti dal RGPD, dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti con modalità cartacee, informatizzate

e telematiche.

2. L'esercizio delle competenze assegnate dalle norme vigenti al titolare è attribuito dal Sindaco, con proprio provvedimento, al Dirigente della struttura, di norma titolare di PEG, (di seguito denominati Titolare) cui i dati ed il relativo trattamento afferiscono, in conformità ai principi dell'Ordinamento degli enti locali ed alle scelte fondamentali assunte dal Comune in materia organizzativa.

3. Il Titolare svolge le funzioni previste dalle disposizioni di legge e di regolamento, sulla base delle direttive impartite dalla Giunta, anche in materia di sicurezza, attraverso il presente Documento, nonché, considerate le caratteristiche organizzative dell'Ente, attraverso le determinazioni che il singolo Dirigente di Settore, in quanto titolare del trattamento dei dati, deve adottare in materia di:

- registro dei trattamenti, secondo lo schema allegato "A"
- distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati ovvero nomina dei Responsabili dei trattamenti interni ed esterni e dei soggetti autorizzati al trattamento (d'ora innanzi incaricati)
- valutazioni di rischi particolari che incombono sui dati
- misure ulteriori da adottare, aggiuntive rispetto a quelle indicate nel presente Documento per garantire l'integrità e la disponibilità dei dati

4. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.

In particolare:

- fornisce all'interessato l'informativa d cui agli artt. 13 e 14 del RGPD

- risponde alle richieste pervenute dagli interessati per l'esercizio dei diritti ad essi riconosciuti dalle disposizioni vigenti. Si applicano al riguardo, laddove non diversamente normato, le disposizioni di cui al Regolamento comunale sull'attività e sui procedimenti amministrativi;

- nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, effettua una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 del RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento;

- designa i Responsabili interni del trattamento nelle persone dei Dirigenti, dei Responsabili, delle Posizioni Organizzative e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza, secondo lo schema allegato "B";

- autorizza ed impartisce adeguate istruzioni per iscritto ai dipendenti che accedono e trattano dati che afferiscono al proprio Settore;

- nomina quale Responsabile esterno del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali, secondo lo schema allegato " C";

- provvede alla notifica della violazione dei dati personali ("*data breach*") all'Autorità Garante Privacy senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui ne è venuto a conoscenza, ove ritenga probabile che, dalla suddetta violazione, possano derivare rischi per i diritti e le libertà degli interessati;

- predispone l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente*;*

- cura la formazione dei propri dipendenti avvalendosi, se lo ritiene opportuno, della collaborazione dell'ufficio che si occupa dell'organizzazione dell'attività formativa;

5. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento (contitolarità), l'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dal diritto nazionale; l'accordo può individuare un punto di contatto comune per gli interessati.

4. Responsabili interni dei trattamenti

1. Il Titolare nomina, con apposito atto, Responsabile del trattamento, sulla base dei necessari requisiti di esperienza, capacità e affidabilità, i Dirigenti, le Posizioni Organizzative e i Funzionari delle singole strutture in cui si articola il settore, che, ai sensi della normativa vigente in materia di privacy, offrano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento soddisfi i requisiti previsti dalla normativa vigente in materia di riservatezza e garantisca la tutela dei diritti degli interessati, secondo lo schema allegato "B".

2. Ogni responsabile del trattamento adempie a quanto disposto dal Titolare, organizza e coordina l'attività degli incaricati e vigila sul fatto che essi operino nel rispetto della legge, nonché dei regolamenti, delle disposizioni, delle procedure e delle istruzioni impartite in materia di protezione dei dati personali.

3. In particolare, il Responsabile :

• procede, d'intesa con il Titolare, alla nomina dei soggetti autorizzati al trattamento;

• verifica che siano rilasciate le informative;

• controlla che siano osservate le misure tecniche e organizzative di sicurezza adottate dall'Ente;

• verifica che siano osservate le disposizioni relative all'esercizio dei diritti dell'interessato.

4. Il Responsabile è tenuto altresì a:

• riferire tempestivamente al Titolare, per quanto di loro competenza, le condizioni o le problematiche che siano suscettibili di rendere difficile o pregiudicare la gestione o l'espletamento delle attività nel rispetto della legge e delle disposizioni del sistema di protezione dei dati personali ed, in particolare, qualsiasi elemento oggettivo o soggettivo che abbia compromesso o possa compromettere la sicurezza, la correttezza e la legittimità dei trattamenti anche in ambito informatico;

• fornire agli incaricati ogni chiarimento necessario o utile alla migliore attuazione e/o gestione del sistema di protezione dei dati personali;

• riferire tempestivamente al Titolare eventuali violazioni della legge e/o del sistema di protezione dei dati personali di cui viene a conoscenza;

• interagire con il Responsabile per la protezione dei dati, laddove richiesto, dandone informazione al Titolare .

5. Incaricati

1. Tutti i dipendenti che, nello svolgimento delle proprie mansioni, hanno accesso a dati personali devono essere autorizzati al trattamento.

2. L'autorizzazione al trattamento dei dati personali deve risultare da un atto di incarico esplicito secondo la schema allegato "D"

3. Ogni soggetto autorizzato al trattamento (d'ora innanzi denominato incaricato) è tenuto ad effettuare esclusivamente le operazioni e i trattamenti individuati nel predetto incarico e non può procedere ad operazioni e/o trattamenti diversi senza una nuova autorizzazione scritta al trattamento.

4. Ciascun incaricato è tenuto, in particolare:

• ad eseguire o applicare le disposizioni impartite;

• osservare scrupolosamente le misure tecniche e organizzative di sicurezza adottate e le altre misure definite dal Titolare;

5. Per quanto concerne le misure di sicurezza per i trattamenti mediante personal computer ciascun incaricato è edotto che:

• ad esso sono associate delle credenziali di autenticazione, comprensive di una parola chiave (password) che deve, con le opportune cautele, mantenere segreta;

• deve essere assicurata la custodia e la riservatezza dei dispositivi di autenticazione per il trattamento con l'ausilio di strumenti elettronici, e non deve essere lasciato incustodito e accessibile lo strumento elettronico durante una seduta di trattamento, anche in caso di assenza temporanea dall'ufficio (es. pausa caffè) in particolare negli orari di accesso agli uffici da parte del pubblico esterno. In questo caso bisogna accertarsi che il PC sia spento o

disconnesso o, in alternativa, oscurato con modalità salvaschermo (cd. screen-saver) dotata di password.

Per i pc a dominio, la modalità salvaschermo con password, viene attivata automaticamente, e lo schermo viene oscurato dopo 10 minuti di non utilizzo.

6. Per quanto riguarda invece i trattamenti senza strumenti elettronici, ciascun incaricato è tenuto a:

• utilizzare la documentazione contenente dati personali in modo da non renderli visibili o accessibili ai soggetti non autorizzati, durante le attività di trattamento e nelle pause dalle medesime; una particolare cautela è imposta per il caso che i documenti contengano dati particolari, sensibili e/o giudiziari;

• riporre e custodire i documenti nei luoghi/schedari predisposti dopo la conclusione delle singole operazioni di trattamento, in particolare facendo uso delle serrature a disposizione per le banche dati che contengano dati sensibili e/o giudiziari;

• in ogni caso, a non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati;

• assicurarsi, al termine della giornata lavorativa, che ogni documento ad esso affidato contenente dati personali sia custodito e protetto da accessi non autorizzati, il ché implica l'uso di serrature relative agli arredi/schedari e la custodia delle chiavi in luogo idoneo – eventualmente concordato con i colleghi di ufficio - ovvero la chiusura stessa della stanza – qualora ciò non osti ad altre attività necessarie.

7. L'incaricato è altresì edotto che è suo compito e responsabilità:

• trasmettere senza ritardo al Responsabile del trattamento le richieste degli interessati relative all'esercizio dei diritti di cui all'art.15 e seguenti del RGPD, accertando l'identità del richiedente e/o il titolo in base al quale abbia effettuato la richiesta;

• eseguire le disposizioni del Titolare e del Responsabile e collaborare con il medesimo nelle pratiche di riscontro/risposta agli interessati;

• astenersi da fornire telefonicamente, a mezzo fax o in qualunque altro modo – anche a fronte delle richieste relative all'esercizio dei diritti di cui al succitato art.15 e seguenti del RGPD - dati di qualunque tipo senza specifica autorizzazione e senza l'identificazione del richiedente;

• partecipare, quando richiesto, alle riunioni convocate dal Titolare o dal Responsabile per qualunque esigenza relativa alla gestione del sistema di protezione dei dati personali e per le

attività di formazione/aggiornamento;

• operare nelle attività di trattamento dei dati con solerzia e scrupolo;

• interagire con il Responsabile per la protezione dei dati, laddove richiesto.

PARTE II - SICUREZZA DEI DATI PERSONALI

6. Disposizioni generali

1. Le misure tecniche ed organizzative di sicurezza poste in atto per ridurre i rischi del trattamento dei dati personali assicurano la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico (Continuità Operativa).

In fase di sviluppo, progettazione, selezione e utilizzo di nuove applicazioni, servizi, prodotti che trattano dati personali, verrà richiesto che le software house provvedano alla cifratura e pseudonomizzazione dei dati nell'ottica del principio di privacy by design.

E' in programma l'implementazione di tecnologie e procedure tecnico/organizzative per garantire il ripristino e la disponibilità dei dati in caso di incidente fisico che comporti la perdita del Data Center, procedure che andranno verificare e valutare regolarmente al fine di garantire la sicurezza dei trattamenti (Disaster Recovery).

E' in corso l'analisi per la definizione di una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Costituiscono misure tecniche ed organizzative:

- le misure contenute nel presente Documento;

- la mappatura dei processi attraverso il Registro dei trattamenti. Ogni dirigente di Settore, in qualità di Titolare, approva con propria determinazione, secondo lo schema allegato al presente Documento sotto la lettera "A", il Registro dei trattamenti e ne cura la regolare tenuta e l'aggiornamento;

- le eventuali ulteriori soluzioni di riduzione dei rischi adottate da ciascun Titolare;

- l'adozione di adeguate misure di sicurezza nel caso sia richiesta la valutazione d'impatto ai sensi dell'art.35 del RGPD;

- le istruzioni fornite a chi ha accesso ai dati personali e la sensibilizzazione e la formazione dei soggetti che, a diverso titolo, vengono coinvolti nel trattamento dei dati personali, in qualità di responsabili , autorizzati al trattamento , amministratori di sistema;

- la definizione, formalizzazione e implementazione di processi e regole connessi alla protezione dei dati personali quali la gestione delle misure di sicurezza e dei diritti degli interessati;

- l'adeguamento della documentazione esistente alle disposizioni normative vigenti (ad esempio informative, clausole contrattuali);

- la definizione di un sistema di controllo delle vulnerabilità dei sistemi e delle applicazioni e delle correzioni necessarie, nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT di cui all'art.1 del presente Documento;

- i sistemi di autenticazione; i sistemi di autorizzazione; i sistemi di protezione (antivirus; firewall; antintrusione; altro);

- le misure antincendio; i sistemi di rilevazione di intrusione; i sistemi di sorveglianza; i sistemi di protezione con videosorveglianza; la registrazione degli accessi; le porte, armadi e contenitori dotati di serrature e ignifughi; i sistemi di copiatura e conservazione di archivi elettronici; le altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

3. Il Comune è inoltre 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 Dirigente di Settore individuare, volta per volta, i casi in cui è necessario o opportuno che documenti, atti, informazioni del proprio Settore, 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 Dirigente di Settore, nei casi sopra indicati, dovrà concordare con i Sistemi informativi 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).

È in corso l'analisi per giungere ad una soluzione tecnica di integrazione della procedura al fine di pervenire all'automatica defissione dei dati alla scadenza prevista dalle disposizioni di legge.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali potrà essere dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. I nominativi ed i dati di contatto del Titolare, e del Responsabile della protezione dati sono pubblicati nella sezione "privacy"del sito istituzionale del Comune e nella sezione "Amministrazione Trasparente".

7. Analisi dei rischi

1. L'efficace protezione dei dati personali è perseguita sia al momento di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi, prodotti che comportano il trattamento di dati personali (privacy by design), sia all'atto del trattamento, garantendo che siano trattati, per impostazione predefinita (privacy by default) solo i dati necessari per ogni specifica finalità di trattamento in relazione, ad esempio, alla quantità di dati personali raccolti, alla portata del trattamento, al periodo di conservazione, all'accessibilità.

2. Le misure tecniche ed organizzative progettate e realizzate assicurano un adeguato livello di sicurezza bilanciando, da un lato, lo stato dell'arte, i costi di attuazione, la natura, l'oggetto, il contesto e le finalità del trattamento e, dall'altro, i rischi che presentano i trattamenti e la natura dei dati personali da proteggere.

3. Ferma restando la facoltà dei dirigenti di settore di individuare rischi particolari connessi ad alcune tipologie di trattamento da inserire all'interno del Registro dei trattamenti, la sottostante tabella intende offrire un quadro sintetico generale dell'analisi dei rischi presenti nell'Ente, che tiene conto dei seguenti aspetti:

- della probabilità del verificarsi dell'evento;
- dell'eventualità di distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati;
- degli eventuali pregiudizi derivati, dei danni fisici, materiali o immateriali.

Tabella

Fattori di rischio	**Tipologia evento**	**Probabilità di verificazione dell'evento: molto alta/alta/media/bassa/molto bassa**
Sottrazione di credenziali di autenticazione	Evento riconducibile al comportamento degli operatori	Medio/Alta
Carenza di consapevolezza, disattenzione o incuria	"	Medio/Alta (probabilità media, impatto alto, es., cancellazione erronea dati)
Comportamenti sleali o fraudolenti	"	Medio/Bassa
Errore materiale	"	Media
Banca dati residente solo su PC e su supporti removibili contenenti dati	"	Bassa
Azione di virus o di altri programmi dannosi	Evento riconducibile all'uso di strumenti elettronici	Media
Spamming o tecniche di	"	Media

sabotaggio		
Malfunzionamento, indisponibilità, degrado degli strumenti	“	Bassa
Accessi esterno non autorizzato ai dati	“	Medio/Bassa
Accesso interno non autorizzato ai dati	“	Medio/ Bassa
Intercettazione di informazioni in rete	“	Medio/Bassa
Accessi non autorizzati agli uffici	Evento relativo al contesto	Media
Accessi non autorizzati a locali/reparti ad accesso ristretto	“	Bassa
Sottrazione di supporti contenenti dati	“	Bassa
Eventi distruttivi naturali	“	Bassa
Eventi distruttivi artificiali	“	Bassa
Guasti ad impianti (es., elettrico, di climatizzazione, ecc.)	“	Bassa

Eventi riconducibili ai comportamenti degli operatori.

La valutazione “media” e “medio/alta” assegnata a ciascuna delle tipologie di evento riconducibili a fatti “colposi” e la valutazione “medio/bassa” per ciò che concerne invece i fatti “dolosi”, si fonda sulla considerazione che i rischi per la riservatezza, disponibilità e integrità dei dati o delle banche di dati, ad oggi possono assai più facilmente derivare da errori o negligenza degli operatori, legata per lo più a sotto considerazione delle problematiche e della valenza da assegnare alle attività di trattamento dei dati personali, piuttosto che da comportamenti intenzionali degli operatori stessi.

Eventi riconducibili all'uso di strumenti elettronici

Per quanto concerne la presenza di banche dati residenti solo su PC e su supporti removibili contenenti dati, la valutazione è " bassa" in quanto il loro uso è vietato.

Per ciò che concerne l'azione di virus o di altri programmi dannosi, la valutazione è "media" perché tutti i pc sono dotati di programmi antivirus, aggiornati in automatico quotidianamente, ma questi sistemi non sono in grado di bloccare la totalità dei virus presenti in rete.

Quanto a spamming o tecniche di sabotaggio, la probabilità dell'evento è da stimare "media", perché nonostante la presenza di un sistema centralizzato di anti-spamm, esiste sempre la possibilità che alcune e-mail passino attraverso il filtro.

Relativamente a malfunzionamento, indisponibilità, degrado degli strumenti, si segnala che il piano di sostituzione dei PC è in fase avanzata e si sta definendo un piano di aggiornamento tecnologico costante per mantenere un livello di sicurezza adeguato.

Sugli accessi esterni non autorizzati, la rete è protetta da una coppia di Firewall di nuova generazione in grado di bloccare, ed eventualmente segnalare, tentativi di intrusione dall'esterno; mentre le applicazioni sono protette da un Web Application Firewall (WAF) in grado di segnalare e bloccare tentativi di sfruttamento di eventuali vurnerabilità applicative.

Riguardo all'intercettazione di informazioni in rete, si valuta "bassa" la probabilità che possa avvenire in quanto l'accesso agli apparati di rete è protetto da password conosciute solo dagli Amministratori di Sistema, ed il traffico dati risulta criptato tramite protocollo Https.

Eventi relativi al contesto

Per ciò che concerne l'evento "sottrazione di supporti contenenti dati", oltre a valere quanto più oltre indicato riguardo all'accesso alle sedi e uffici, si segnala che il personale ha il dovere di vigilare sull'uso della strumentazione informatica in dotazione e di utilizzarla correttamente. Al riguardo sono state impartite precise istruzioni nel Disciplinare sull'uso degli strumenti di lavoro e la registrazione delle presenze e delle assenze del Comune di Modena. Per questo motivo, la probabilità di verificazione di tale evento è stimata "bassa". Nondimeno i dirigenti di settore sono tenuti a sollecitare periodicamente l'attenzione del personale su questo aspetto.

Si reputa bassa la probabilità di eventi distruttivi naturali, in considerazione della valutazione delle vicende pregresse.

Eventi distruttivi artificiali non si sono mai verificati e comunque anche per essi si prevede, in via preventiva, la costante vigilanza del personale preposto. La probabilità di verificazione dell'evento è per ciò stimata "bassa". Per gli eventi distruttivi naturali e artificiali, si ritiene fondamentale l'attività del Servizio Prevenzione e Protezione che dovrà garantire la protezione delle aree e dei locali, con specifico riferimento ai Piani di Emergenza elaborati per le diverse Strutture Comunali.

Relativamente ai guasti agli impianti (ad esempio guasti all'impianto elettrico), non si segnalano situazione di rischio particolare né si registrano episodi pregressi. La probabilità di verificazione dell'evento è per ciò al momento stimata "bassa".

Relativamente alle misure adottate per ridurre il rischio di perdita dei dati dell'Ente a seguito di eventi naturali e/o artificiali, si rimanda al punto 14 del presente Documento.

Relativamente agli impianti di sicurezza dei Data Center, si rimanda al punto 15 del presente Documento.

8. Quadro riepilogativo dei codici di riferimento per l'individuazione delle misure di sicurezza nel Registro dei trattamenti

Per l'individuazione delle misure di sicurezza tecniche e organizzative, il Registro dei trattamenti fa riferimento ai seguenti codici

1 . Misure organizzative

a. autorizzazione formale al trattamento

b. istruzioni per il trattamento

c. locali chiusi a chiave in assenza dell'incaricato

d. archivi/ contenitori chiusi a chiave in assenza dell'incaricato

e. accessi controllato al di fuori degli orari di apertura

f. accessi videosorvegliati

g. formazione

h. nomina per iscritto del responsabile esterno

i. altro (indicare)

2. Misure tecniche

a. procedura di autenticazione

b. procedura di autorizzazione

c. procedura di modifica credenziali

d. profilazione

e. salva schermo

f. firewall

g. antivirus

h. disaster recovery

i. antivirus

l. intrusion detection

m. vulnerability assesment/ penetration test

n. cifratura dei dati

o. separazione dei dati

p. adozione delle misure minime di sicurezza ICT

q. altro (indicare)

Rispetto alle procedure informatiche in uso presso ciascun Settore, il Titolare, nella propria determinazione, rinvierà ad un Documento predisposto dai Sistemi informativi contenente tutte le necessarie specifiche

9. Formazione

1. Il programma di formazione ha lo scopo di rendere consapevoli i dipendenti delle problematiche inerenti la sicurezza e di responsabilizzarli sulle attività da eseguire. L'attività formativa interessa tutto il personale.

2. Il Settore a cui compete la gestione dei processi di formazione cura la formazione dei nuovi assunti.

3. Ogni Settore deve curare la formazione dei propri dipendenti avvalendosi, se lo ritiene opportuno, della formazione on line e della collaborazione dell'ufficio che si occupa dell'organizzazione dell'attività formativa.

4. I corsi saranno progettati in base alle diverse esigenze e; in generale, non potranno mancare riferimenti a:

- normativa vigente;
- definizione delle responsabilità;
- elenco delle vulnerabilità al fine di acquisire maggiore 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..

10. Accesso alle sedi e uffici

1. L'apertura e la chiusura delle principali sedi e l'accesso agli uffici durante gli orari di apertura al pubblico è affidata agli addetti alla portineria o a personale preposto. Al di fuori degli orari di apertura, l'accesso è consentito tramite badge identificativo personale, e controllato da addetti alla sorveglianza gestiti dal Servizio Finanze, Economato e Organismi partecipati.

Di sera la sorveglianza viene effettuata attraverso un sistema d'allarme gestito dal Settore Lavori Pubblici, Mobilità e Manutenzione urbana e attivato da remoto da parte della ditta addetta al sistema di vigilanza che, in caso di allarme, contatta l'operatore del Comune reperibile di turno e invia una pattuglia con guardia giurata. Sia l'operatore del Comune che gli addetti alla sorveglianza sono in possesso di badge che consente l'accesso alla struttura in qualsiasi orario. Nel caso di segnalazione di guasto al sistema di allarme, gli addetti al sistema di sorveglianza attivano il tecnico della ditta incaricata della manutenzione.

Presso il Settore Lavori Pubblici, Mobilità e Manutenzione urbana è presente una bacheca dove sono custodite le chiavi di accesso dei principali edifici in proprietà o in uso al comune di Modena. La bacheca è custodita in apposito armadio all'interno del locale portineria del settore. Il locale è dotato di proprio sistema di allarme anti intrusione e viene chiuso a chiave tutte le sere alle 18.30. Solo il tecnico di turno di reperibilità ha le chiavi poi per aprire e accedere alla bacheca. Durante il giorno la portineria è aperta ma presidiata da personale del Comune di Modena. Altre copie delle chiavi sono custodite nel caveau degli uffici della ditta incaricata della vigilanza e vengono consegnate alle pattuglie di vigilanza quando montano in servizio in relazione alle zone che controllano.

Le chiavi in bacheca possono inoltre essere consegnate alle imprese che fanno servizi di manutenzione o hanno appalti di lavori in corso con e per il Comune di Modena. In questo caso vengono sempre registrati i dati del referente dell'impresa che ritira le chiavi, compreso il numero di cellulare al quale tale persona può essere contattata per riavere le chiavi stesse in caso di necessità.

Presso il Palazzo Municipale, il Palazzo dei Musei, il Palazzo Margherita, il Parco Archeologico di Montale, il Centro Musica, l'Archivio Stamperia, la Casa protetta Vignolese e il Settore Lavori Pubblici, Mobilità e Manutenzione urbana è installato un sistema di videosorveglianza manutenuto dalla ditta che gestisce il servizio. Le registrazioni vengono prelevate solo da personale addetto al servizio di vigilanza qualora le autorità di pubblica sicurezza ne facciano richiesta. Sono altresì autorizzati all'accesso il direttore per l'esecuzione dell'appalto dei servizi manutenzione impianti di sicurezza, e il responsabile del procedimento.

2. Il Servizio Finanze, Economato e Organismi partecipati provvede altresì 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.

PARTE III - TRATTAMENTO DEI DATI CON STRUMENTI ELETTRONICI

11. Struttura del sistema e protezioni

11.1 Architettura della rete

1. L'Amministrazione si è dotata di una rete in fibra ottica in proprietà, che collega oltre 40 sedi sul territorio comunale, a formare un anello, che consente il funzionamento della rete anche nel caso di guasto su una tratta di collegamento.

2. Su questa rete l'amministrazione veicola i servizi dati e di fonia interna, alcuni servizi sul territorio gestiti dal Comune (es. il sistema di telecamere di video sorveglianza), ed altri gestiti da Lepida SpA (wifi pubblico cittadino).

3. Tutti i dipendenti dotati di PC sono quindi collegati alla rete Intranet, dalla quale possono accedere alle applicazioni dell'Ente; i dipendenti autorizzati accedono ad Internet in un unico punto, filtrati dal sistema di firewall aziendale.

11.2 Sicurezza della rete

1. La rete del Comune è connessa all'esterno attraverso diversi canali di trasmissione dati:

- Collegamento alle rete Internet: questo servizio è fornito dall'operatore pubblico di telecomunicazioni Lepida SpA , società della Regione ER di cui è socio il Comune di Modena;
- Collegamenti su linea telefonica, tramite un access server ridondati;
- Collegamenti GPRS/UMTS, tramite un accesso (APN) dedicato.

2. Attraverso i collegamenti internet è inoltre stato realizzato un sistema di VPN basato su funzionalità del sistema firewall comunale.

Sia quest'ultimo che i collegamenti tramite linea telefonica e APN dedicato, consentono l'accesso alla rete comunale tramite autenticazione con nome utente e password e prevedono la criptatura del traffico dati.

3. Tutti i sistemi elencati afferiscono ad un sistema di firewall, che controlla il traffico dati in base a politiche di sicurezza prestabilite.

11.3 Architettura del Sistema Informatico

1. Banche dati

I dati strutturati delle applicazioni gestionali possono essere memorizzati in:

- banche dati centralizzate, per le applicazioni utilizzate da più utenti

- più raramente, su stazione di lavoro per applicazioni mono-utente

Oltre alle banche dati delle applicazioni gestionali esistono archivi documentali non strutturati, residenti su:

- server centrali (file server/NAS)
- sulle stazioni di lavoro

2. Posta elettronica

Ad ogni dipendente è assegnata una casella individuale; inoltre esistono caselle non nominali corrispondenti a gruppi di lavoro o figure istituzionali.

3. Sistemi di autenticazione

Attualmente sono presenti 2 sistemi centralizzati di autenticazione/autorizzazione:

- Directory server LDAP (Lightweight Directory Access Protocol), utilizzato per autenticare gli utenti di applicativi su ambienti Unix:
  - posta elettronica
  - navigazione internet
  - applicativi su server web
- Dominio Windows Active Directory Active Directory utilizzato per autenticare gli utenti di risorse condivise su rete come:
  - accessi via VPN
  - personal computer a dominio AD
  - cartelle di rete
  - stampanti e multifunzione
  - applicativi su server web

LDAP è l'archivio principale in cui sono memorizzate le informazioni personali e le autorizzazioni all'utilizzo delle procedure applicative.

Sono stati messi a punto meccanismi di aggiornamento e allineamento degli utenti fra i vari sistemi.

- I dati personali degli utenti dipendenti del Comune di Modena presenti su LDAP vengono aggiornati automaticamente estraendoli dagli archivi del Settore Risorse umane e strumentali. Per gli utenti che non sono dipendenti del Comune di Modena i dati vengono inseriti e aggiornati a seguito della comunicazione del Dirigente del Settore titolare della banca dati

- Le modifiche alla password su LDAP vengono riportate automaticamente sul dominio Active Directory

Alcune procedure applicative non utilizzano questi sistemi centralizzati, ma possiedono un proprio sistema interno di autenticazione ed autorizzazione degli utenti, con credenziali specifiche**.**

In questo caso, la password viene impostata dall'utente ed è a suo carico il rispetto delle seguenti indicazioni:

- la password deve essere composta, dove l'applicazione lo consenta, da almeno 8 caratteri
- la password non deve contenere riferimenti agevolmente riconducibili all'incaricato
- nel caso in cui la procedura contenga dati personali e/sensibili, la password dovrà essere modificata almeno ogni tre mesi.

L'autenticazione degli utenti sui personal computer inseriti nel domino AD, avviene tramite l'utilizzo delle credenziali di dominio, mentre per i personal computer non inseriti a dominio, l'autenticazione avviene tramite username e password definite localmente, cioè memorizzate sul pc stesso.

11.4 Sicurezza dei dati

1. 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 dal sistema d'autenticazione centralizzato (LDAP o AD) oppure dalla procedura stessa.

Contestualmente viene verificato se l'utente è autorizzato all'utilizzo della funzionalità richiesta tramite apposita profilazione gestita a livello applicativo.

2. Cartelle di rete centralizzate

I server contenenti cartelle di rete con documenti non strutturati richiedono l'autenticazione e l'autorizzazione dell'utente tramite il dominio Active Directory.

Questa autenticazione avviene in modo trasparente per l'utente (senza la richiesta di ulteriore autenticazioni) se il personal computer è inserito a dominio e, per i personal computer non a dominio, se le credenziali di accesso allo stesso sono uguali a quelle di dominio Active Directory.

3. 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, debbono essere protetti da credenziali di accesso personali, come precedentemente descritto.

Conseguentemente, PC ai quali sia possibile accedere con credenziali generiche (non personali) non debbono contenere banche dati e/o documenti con dati personali e/o sensibili.

12. Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni

12.1 *Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica*

1. Soggetto preposto alla gestione delle credenziali per l'accesso alle banche dati centralizzate che utilizzano i sistemi LDAP o Active Directory è il Responsabile dell'Ufficio Reti Informatiche del Settore a cui compete la gestione del sistema informatico / telematico del Comune.

2. Il Titolare, tramite apposita procedura informatica, può verificare gli utenti autorizzati ad accedere alle banche dati di cui ha titolarità, e le autorizzazioni in possesso dei dipendenti del proprio settore.

3. Il soggetto preposto provvederà con periodicità semestrale, ad inviare una mail di promemoria ad ogni Titolare con le informazioni necessarie alle verifiche suddette.

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

5. 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.

12.2 Trattamento dei dati personali affidati ai lavoratori

A) Assegnazione delle credenziali di autenticazione

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

2. Nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT per la Pubbliche Amministrazioni di cui all'art.1 del presente Documento, le credenziali sono nominative e riconducibili ad una sola persona.

3. In caso di assunzione di un nuovo lavoratore, il Dirigente del Settore competente o il responsabile del trattamento dei dati da lui delegato richiede al preposto alla gestione, attraverso l'apposita procedura informatica, 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 nelle banche dati necessarie e comunica le credenziali all'utente in modo riservato. È a cura del lavoratore sostituire la password provvisoria con quella definitiva.

B) Assegnazione delle autorizzazioni

1. Per poter accedere, a qualsiasi titolo, alle applicazioni ed alle banche dati del Comune occorre essere autorizzati.

2. 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 dei dati d'intesa con il titolare del trattamento, vale a dire il Dirigente del Settore.

3. La competenza alla richiesta, revoca, modifica delle autorizzazioni è del Dirigente del Settore di appartenenza del lavoratore il quale può delegarla al responsabile al trattamento dei dati.

Accesso ad applicazioni e banche dati del Settore di appartenenza

Il Dirigente del Settore di appartenenza/responsabile delegato sulla base dell'incarico conferito al lavoratore, comunica al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, 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.

Accesso ad applicazioni e banche dati di altri Settori.

Nel caso che il lavoratore necessiti di accedere a banche dati di un altro Settore, l'incarico dovrà essere dato congiuntamente dal Dirigente del Settore di appartenenza e dal Dirigente di Settore titolare della banca dati utilizzata.

Una volta conferito l'incarico, il Dirigente del Settore di appartenenza/ responsabile delegato richiede al preposto alla gestione, attraverso l'apposita procedura informatica, l'abilitazione del lavoratore alle banche dati richieste, attestando che il Dirigente del Settore titolare della banca dati ne è stato informato.

Il preposto alla gestione procede con le modalità indicate al paragrafo precedente.

Cessazione del rapporto di lavoro

Dopo 90 giorni dalla data di cessazione del rapporto lavorativo, il preposto alla gestione delle credenziali, attraverso una procedura automatica, ricava il nominativo del lavoratore cessato, ne revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica, e ne informa il responsabile informatico dell'applicazione.

Nel caso di prestazione occasionale, di tirocinio formativo, di incarico professionale ed in genere in tutti i casi in cui non è possibile ricavare l'informazione dell'avvenuta cessazione

in modo automatico dalla Banca dati centralizzata del Settore a cui compete la gestione del personale, spetta al Dirigente del Settore competente/ responsabile delegato comunicare tempestivamente al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, 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, attraverso l'apposita procedura informatica, il Dirigente del Settore competente e il responsabile informatico dell'applicazione. Prima della cessazione del rapporto di lavoro, il lavoratore deve eliminare i documenti e le e-mail che non siano di interesse del Settore, autorizzando attraverso l'apposita procedura informatica, il Dirigente ad accedere ai documenti ed alle e-mail rimanenti. Il Dirigente di Settore/ responsabile delegato deve prontamente avvisare il soggetto preposto alla pulizia o recupero delle banche dati di cui al punto 13.1 concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti.

Nel caso in cui, per esigenze contingenti, non sia stata rilasciata la liberatoria, il Dirigente di Settore/ responsabile delegato richiede ed autorizza l'intervento del tecnico dell'Ufficio reti Informatiche, che avverrà, ove possibile, alla presenza dell'interessato. Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente di Settore/ responsabile delegato, che ne informa l'interessato alla prima occasione utile, qualora non presente.

Nel caso in cui si provveda al ritiro della stazione di lavoro, i dati legati al profilo del lavoratore verranno resi indisponibili dopo averne trattenuto una copia. Entro un mese il Dirigente di Settore/ responsabile delegato può richiedere il recupero di eventuli dati presenti sul pc 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 dati del pc mentre le e-mail verranno conservate sino ad 1 anno dalla cessazione del dipendente.

Trasferimento del lavoratore

Nel caso di trasferimento presso un altro Settore di un lavoratore, il preposto alla gestione delle credenziali, dopo aver rilevato l'informazione attraverso la Banca dati centralizzata del Settore a cui compete la gestione del personale, provvede a revocare tutte le autorizzazioni all'accesso del lavoratore, ad eccezione dell'indirizzo di posta elettronica, e ne informa, attraverso l'apposita procedura informatica, il responsabile informatico dell'applicazione. Su richiesta del Dirigente di Settore il lavoratore trasferito deve reindirizzare al Settore di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo.

Il Dirigente del Settore 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 altro Settore, con le stesse modalità previste nel caso di nuova assunzione.

Nel caso di trasferimento di un lavoratore nell'ambito dello stesso Settore, il Dirigente di Settore/ responsabile delegato, sulla base del nuovo incarico al trattamento dei dati conferito

e delle competenze a quest'ultimo attribuite, comunica al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, le autorizzazioni all'accesso da revocare e le nuove applicazioni, anche relative all'accesso a banche dati di un altro Settore, alle quali il lavoratore è autorizzato ad accedere. Il preposto alla gestione delle credenziali disabilita le autorizzazioni all'accesso e per le nuove abilitazioni procede con le modalità previste nel caso di nuova assunzione informando, attraverso l'apposita procedura informatica, il Dirigente di Settore e il responsabile informatico dell'applicazione.

Nel caso che il trasferimento del lavoratore (ad un altro Settore o nell'ambito dello stesso Settore) comporti il contemporaneo trasferimento del PC, il lavoratore è tenuto a consegnare al Dirigente i dati di interesse del Settore e successivamente a rimuoverli dalla propria stazione di lavoro. Su richiesta del Dirigente di Settore il lavoratore trasferito deve altresì reindirizzare al Settore di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo.

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.

12.3. Amministratori di Sistema

1. Il Dirigente del Settore a cui compete la gestione del sistema informatico / telematico nomina i dipendenti dei proprio settore incaricati a svolgere le attività di Amministratore di Sistema.

2. Nel caso in cui l'amministratore di sistema appartenga ad un altro Settore, fatta salva una diversa pattuizione, la designazione da parte del Dirigente del Settore a cui compete la gestione del sistema informatico / telematico avviene previa richiesta del Dirigente del Settore di appartenenza che ne attesta le caratteristiche di esperienza, capacità e affidabilità.

3. Nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT di cui all'art.1 del presente Documento, ad essi vengono assegnate doppie credenziali, una per l'uso non amministrativo (es: posta, cartelle di rete, VPN, procedure informatiche del comune, etc.) e una per le attività amministrative (server, db, etc.). Le credenziali amministrative sono composte dallo userd dell'utente preceduto da "a-" con password diversa rispetto alle credenziali non-amministrative.

4. La disattivazione/revoca, la scadenza, il recupero e il cambio password sono le medesime dell'utente non amministratore. L'avviso di scadenza della password viene mandata tramite mail alla casella dell'utente, e tramite SMS se è stato fornito il numero di cellulare durante la procedura di cambio password.

5. Gli estremi identificativi delle persone fisiche designate, con l'indicazione delle funzioni ad esse attribuite, è riportato in un elenco agli atti del settore stesso. Con cadenza annuale il Dirigente del Settore a cui compete la gestione del sistema informatico / telematico 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, e provvede alla pubblicazione sulla intranet dell'elenco aggiornato degli Amministratori di Sistema che trattano dati relativi al personale.

6. Il Settore a cui compete la gestione del sistema informatico / telematico 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, tramite l'utilizzo di uno specifico strumento informatico**.**

12.4. Trattamento dei dati personali affidati a soggetti esterni

1. Sono considerati soggetti esterni tutti quei soggetti che non rientrano nell'art.12.2 (a puro titolo esemplificativo: società, enti, consorzi, professionisti, soggetti pubblici o gestori di pubblici servizi).

2. La titolarità del trattamento dei dati resta in capo al Comune.

3. Il Dirigente del Settore titolare della banca dati, congiuntamente al Dirigente del Settore/ Servizio contraente, nomina il soggetto esterno responsabile del trattamento dei dati secondo l'allegato modello "C" che potrà essere modificato o integrato in relazione alle specifiche esigenze del Settore.

Nel caso in cui l'oggetto del contratto o della convenzione comporti l'utilizzazione di applicazioni o banche dati di competenza di più Settori, la designazione del responsabile dovrà essere sottoscritta congiuntamente dal Dirigente del Settore titolare della banca dati e dai Dirigenti delle banche dati interessate.

4. All'inizio della collaborazione il soggetto esterno responsabile del trattamento fornisce al Responsabile dei Sistemi informativi l'elenco degli incaricati al trattamento dei dati da lui nominati per i quali si richiede il rilascio delle credenziali.

5. Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità non superiore ai 24 mesi, se comunicato. In caso contrario il periodo di validità delle credenziali è di 12 mesi. Almeno 60 giorni prima della scadenza il preposto alla gestione delle credenziali comunica al Dirigente di Settore e a tutti gli abilitati alla procedura informatica di gestione "scadenza utenti esterni", tramite e-mail che, scaduto il periodo di validità, le credenziali dell'utente, salvo diversa comunicazione, saranno disabilitate. Trascorsi 30 giorni dalla scadenza del periodo di validità delle credenziali, senza che sia pervenuta una diversa comunicazione da parte del Dirigente di Settore, l'utente verrà dimissionato.

6. L'utente esterno che utilizza un PC di proprietà del Comune, assegnato a titolo di comodato d'uso gratuito o ad altro titolo, prima della cessazione a qualsiasi titolo del suo incarico, deve eliminare dallo stesso i documenti, e le e-mail dalla propria casella di posta, che non siano di interesse del Settore, autorizzando per iscritto il Dirigente ad accedere ai documenti ed alle e-mail rimanenti. Il Dirigente di Settore/ responsabile delegato deve prontamente avvisare il soggetto preposto alla pulizia o recupero delle banche dati di cui al punto 13.1 concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti. Nel caso in cui, per esigenze contingenti, non sia stata rilasciata la liberatoria, il Dirigente di Settore/ responsabile delegato richiede ed autorizza l'intervento del tecnico dell'Ufficio Reti Informatiche, che avverrà, ove possibile, alla presenza dell'interessato Questo intervento verrà documentato mediante apposito verbale redatto a

cura del Dirigente di Settore/ responsabile delegato che ne informa il lavoratore alla prima occasione utile.qualora non presente. L'utente esterno che utilizzi un PC non di proprietà del Comune dovrà provvedere a trasmettere al Dirigente tutti i documenti e le e.mail di interesse del Settore, senza procedere a duplicazioni di dati e programmi, se non espressamente autorizzato.

7. Nel caso in cui si provveda al ritiro della stazione di lavoro i dati legati al profilo dell'utente esterno verranno resi indisponibili dopo averne trattenuto una copia. Entro un mese il Dirigente di Settore/ responsabile delegato può richiedere il recupero delle banche dati e delle e.mail giacenti nella casella di posta disabilitata, esibendo la relativa autorizzazione dell'utente esterno. Trascorso tale periodo il preposto provvederà alla eliminazione definitiva dei suddetti dati.

12.5. Accesso alle banche dati

1. L'accesso telematico alle banche dati del Comune di Modena è consentito alle amministrazioni pubbliche e ai soggetti gestori o concessionari di servizi pubblici esclusivamente per finalità istituzionali.

2. L'accesso dovrà avvenire attraverso convenzione sottoscritta dal Dirigente del Settore competente e dal rappresentante della pubblica amministrazione/gestore o concessionario di servizi pubblici.

12.6 . Amministratori di sistema esterni.

1. Il Responsabile esterno del trattamento dei dati nomina l'Amministratore di Sistema e ne comunica il nominativo, i dati di riferimento e le funzioni ad esso attribuite al Titolare e ai Sistemi informativi.

2. In analogia a quanto previsto all'art.12.3 e nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT di cui all'art.1 del presente Documento, agli Amministratori di Sistema Esterni vengono assegnate doppie credenziali, una per l'uso non amministrativo es: posta, cartelle di rete, VPN, procedure informatiche del comune, etc.) e una per le attività amministrative (server, db, etc.). Le credenziali amministrative sono composte dallo userd dell'utente preceduto da “a-” con password diversa rispetto alle credenziali non-amministrative.

3. La disattivazione/revoca, la scadenza, il recupero e il cambio password sono le medesime dell'utente non amministratore. L'avviso di scadenza della password viene mandata tramite mail alla casella dell'utente, e nel caso i cui non sia dotato di e-mail, tramite SMS se è stato fornito il numero di cellulare durante la procedura di cambio password.

4. L'elenco degli Amministratori di Sistema Esterni viene mantenuto aggiornato a cura di ciascun Responsabile Esterno che si impegna a comunicare ogni variazione al Dirigente che lo ha nominato e al Dirigente del Settore a cui compete la gestione del sistema informatico / telematico

12.7 . Modalità di gestione delle password

1. Le password utilizzate nei sistemi di autenticazione LDAP e Active Directory sono assegnate dal preposto alla gestione delle credenziali all'atto della creazione delle credenziali stesse, sono identiche 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.

La modifica della password LDAP comporta la modifica automatica anche della password Active Directory e dell'utente Proxy Oracle se l'utente è abilitato.

2. Sulle stazioni non definite nel dominio Active Directory viene creato un profilo con lo stesso userid che l'utente ha sui sistemi centralizzati di autenticazione ma con passwod provvisoria. Sulle stazioni definite in Active Directory il cambio di password è gestita automaticamente. Il dipendente ha l'obbligo di impostare la password seguendo la procedura di cambio password nel rispetto della normativa vigente.

3. Le password degli utenti non Amministratori gestite tramite il sistema LDAP sono composte da 8 caratteri e scadono automaticamente ogni tre mesi.

4. L'avviso di scadenza della password viene mandata tramite mail alla casella dell'utente, e nel caso i cui non sia dotato di e.mail, tramite SMS se fornito durante la procedura di cambio password.

5. Per motivazioni tecniche è opportuno avere un'unica password per l'accensione del PC, per l'accesso ad internet e per l'apertura della posta elettronica.

6. Il lavoratore, qualora dimentichi la password d'accesso al proprio PC, dovrà rivolgersi al lavoratore da lui delegato alla custodia delle password (si veda articolo 13.3) o, in alternativa, al servizio di assistenza che si recherà sul posto e consentirà all'utente l'accesso al PC allo scopo di impostare una nuova password se la stazione di lavoro non è definita in dominio Active Directory.

7. Qualora invece l'utente LDAP o l'utente la cui stazione di lavoro sia definita in Active Directory dimentichi la propria password, dovrà:

- rivolgersi al lavoratore da lui delegato (si veda articolo 13.3);

oppure:

- rivolgersi all'Ufficio Reti Informatiche che provvederà, previa identificazione personale, a fornire al lavoratore o a un suo delegato, una password provvisoria che consentirà di accedere alla procedura di modifica ed ottenere quella definitiva;

oppure:

- utilizzare l'apposita procedura informatica che consente di ottenere, tramite SMS inviato ad un cellulare precedentemente comunicato dal lavoratore, un codice d'accesso con cui ottenere una password provvisoria che consentirà poi di accedere alla procedura di modifica ed ottenere quella definitiva.

8. 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 articolo 12.8

9. Un utente che non sia stato disabilitato può, in qualsiasi momento, modificare la propria password LDAP autenticandosi con userid e vecchia password (valida **solo** per questa funzione anche se scaduta): la nuova password verrà scelta dall'utente tra quelle proposte dal sistema .

10. Ogni incaricato che riceve le proprie password ne è direttamente responsabile. Fatta eccezione per quanto previsto dall'articolo 13.3, 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.

11. Le password degli Amministratori di Sistema, nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT di cui all'art.1 del presente Documento, hanno lunghezza di 14 caratteri, e scadono automaticamente ogni 3 mesi.

12. Per gli altri aspetti, valgono le regole descritte per le password degli utenti non-Amministratori.

12.8 Disattivazione credenziali per disuso.

1. Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione

Per riattivare le credenziali, l'utente dovrà rivolgersi all'Ufficio Reti Informatiche che provvederà, previa identificazione personale, 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 .

13 . Modalità di gestione delle stazioni di lavoro

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

1.Preposto alla pulizia o recupero delle banche dati su PC è il Responsabile dell'Ufficio Reti Informatiche del Settore a cui compete la gestione del sistema informatico / telematico del Comune che provvederà anche avvalendosi di società esterne.

13.2 Programmi antivirus

1. Su tutti i PC, nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT di cui all'art.1 del presente Documento, è installato un programma antivirus che viene aggiornato periodicamente in modo automatico, tramite l'accesso in rete al Server di gestione antivirus; l'antivirus installato sui singoli PC controlla in tempo reale i documenti utilizzati, mentre sui

server è presente un sistema specifico anti-malware.

2. I Server di Gestione Antivirus e Antimalware si aggiornano in modo automatico.

Il software antivirus provvede automaticamente ad effettuare una scansione completa dei dischi interni delle stazioni di lavoro una volta alla settimana.

13. 3 Interventi di accesso o manutenzione del PC

Richiesta di accesso

1. In caso di assenze programmate dal lavoro (per ferie o per qualsiasi altro motivo) il lavoratore attiva preventivamente sulla mail il sistema di risposta automatica. Il messaggio di risposta predefinito deve essere personalizzato dall'utente e potrà indicare l'indirizzo di posta elettronica di un altro utente al quale il mittente può fare riferimento in caso di comunicazioni urgenti.In caso di assenze dal lavoro non programmate, l'utente attiva da remoto, se possibile, il sistema di risposta automatica della propria casella di posta elettronica. 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 il Dirigente di Settore, sulla base delle scelte operative/organizzative effettuate, valuta i casi in cui il 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 Dirigente del Settore o del responsabile del trattamento, accede ai dati e alle procedure nonché ai messaggi di posta elettronica del lavoratore assente provvedendo a inoltrare al Dirigente del Settore o al responsabile da quest'ultimo indicato quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa .

2. Dell'attività compiuta è redatto apposito verbale a cura del Dirigente/responsabile che ne informa il lavoratore assente alla prima occasione utile.

3. Nel caso in cui non sia stato delegato alcun lavoratore oppure nel caso in cui anche il lavoratore delegato non sia presente, il Dirigente Responsabile di Settore/ responsabile delegato richiede ed autorizza l'intervento dei tecnici dell'Ufficio Reti Informatiche , che ne permettono l'accesso per il tempo necessario. Questo intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente Responsabile del Settore/ responsabile delegato e comunicato al lavoratore alla prima occasione utile.

4. Gli interventi dei tecnici dell'Ufficio Reti Informatiche 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.

5. Per ridurre le problematiche sopra descritte, resta valida l'indicazione d'utilizzare preferibilmente le cartelle condivise che, inoltre, sono garantite da copie di sicurezza effettuate almeno giornalmente.

Interventi di Manutenzione

1. Quando per un PC occorre fare un intervento di manutenzione, ordinaria o straordinaria, sul loco o in laboratorio, sarà cura del lavoratore concordare modi e tempi di intervento con i tecnici addetti.

2. 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.

3. 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.

13.4 Società esterna a cui compete la manutenzione e l'assistenza

1. Il Dirigente del Settore a cui compete la gestione del sistema informatico / telematico nomina la società che effettua la manutenzione hardware e software delle postazioni di lavoro, come Responsabile esterno del trattamento dei dati, utilizzando l'allegato modello "C" il quale andrà integrato con una specifica assunzione di impegno da parte del responsabile 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) usare riservatezza su dati ed informazioni addivenuti in loro possesso

d) trasmettere al Dirigente del Settore a cui compete la gestione del sistema informatico / telematico, all'inizio della collaborazione l'elenco degli incaricati al trattamento e successive variazioni

e) trasmettere tempestivamente al Dirigente che lo ha nominato responsabile esterno del trattamento e al Dirigente del Settore a cui compete la gestione del sistema informatico / telematico il nominativo degli Amministratori di Sistema ed ogni eventuale variazione di questi incarichi.

13.5 Dismissione delle stazioni di lavoro

1. In caso di dismissione di PC, il Dirigente che ha in carico la stazione di lavoro deve prontamente 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.

2. 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.

14. Salvataggio dei dati

1.Ove tecnicamente possibile, le banche dati devono risiedere unicamente su server. Il salvataggio delle banche dati esistenti sui server è in carico all'Ufficio Reti Informatiche.

2. Sui sistemi centralizzati, nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT di cui all'art.1 del presente Documento, vengono fatte copie almeno quotidiane degli archivi documentali e delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente.

Le copie vengono effettuate su una libreria di backup presso il Data Center della sede della Polizia Municipale.

L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dagli operatori di sala macchine.

3. Ogni singolo lavoratore è responsabile del salvataggio degli archivi esistenti sul proprio PC.

4. E' vietata la creazione di banche dati residenti solo su pc.

5. E' vietato l'uso di chiavette USB e altri dispositivi mobili per la raccolta e conservazione di dati personali

6. Le copie di salvataggio effettuate dai singoli utenti, possono essere archiviate o distrutte, ma in ogni caso non possono essere usate per la trasmissione dei dati all'esterno.

15 . Locali

1. Il Data Center dell'Ufficio Reti Informatiche dove risiedono fisicamente i server e le librerie a dischi magnetici su cui sono memorizzati i dati dell'Ente, è dotata di impiantistica tale da garantire la sicurezza fisica dell'hardware, sia delle banche dati:

1. porta d'ingresso ad accesso controllato da videocitofono;
2. stabilizzatore di temperatura per i locali;
3. gruppo elettrogeno esterno e doppio gruppo di continuità e di stabilizzazione della corrente;
4. impianto di rilevamento fumi e spegnimento automatico in caso di incendio, collegato con la sede di una società di sicurezza e pronto intervento;
5. impianto antintrusione collegato con la sede di una società di sicurezza e pronto intervento.

2. Il Data Center secondario sita presso la sede della Polizia Municipale in cui risiede la libreria a dischi magnetici utilizzata per le copie di backup, è dotata di:

1. porta d'ingresso al locale e sistema di videosorveglianza controllato dalla centrale operativa PP.MM.

2. stabilizzatore di temperatura per i locali;
3. gruppo elettrogeno esterno e gruppo di continuità e di stabilizzazione della corrente.

16 . Uso del Computer

1. Il PC non deve essere lasciato incustodito.

2. In caso di assenza anche temporanea dall'ufficio, l'utente attivo al momento deve essere spento o disconnesso o, in alternativa, deve essere oscurato con modalità salvaschermo dotata di password . Per i pc a dominio, la modalità salvaschermo con password, viene attivata automaticamente, e lo schermo viene oscurato dopo 10 min. di non utilizzo.

3. Il Dirigente di Settore/ responsabile delegato può impartire ulteriori istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro.

ALLEGATO A

SCHEDA REGISTRO DEI TRATTAMENTI
SETTORE
TITOLARE/ CONTITOLARE *(nome, indirizzo, telefono, mail, PEC)*
RESPONSABILE DELLA PROTEZIONE DEI DATI (nome, indirizzo, telefono, mail, PEC)
DATA DI CREAZIONE
DATA ULTIMO AGGIORNAMENTO

tipologia di trattamento	finalità e basi legali del trattamento	categorie di interessati	categorie di dati personali	categorie di destinatari (indicare anche eventuali responsabili esterni e titolari a cui si sono comunicati i dati)	trasferimento dati verso paesi terzi o organizzazioni internazionali	termini ultimi di cancellazione previsti	misure di sicurezza tecniche e organizzative

FINALITÀ E BASI LEGALI DEL TRATTAMENTO

Indicare:

– legittimo interesse pubblico concretamente perseguito

– norma di legge o di regolamento che legittima il trattamento

– eventuale valutazione di impatto effettuata

– per i dati particolari, indicare una delle condizioni di cui all'art.9 del RGDP

– nel caso di trattamento relativo a condanne penali e reati, la specifica normativa che autorizza il trattamento

CATEGORIE DI INTERESSATI

Indicare la tipologia di persone fisiche a cui si riferiscono i dati personali (es. dipendenti, utenti, fornitori …)

CATEGORIE DI DATI PERSONALI

Indicare la tipologia di dati personali (es. dati anagrafici, dati che rivelano l'origine razziale o etnica, dati che rivelano le opinioni politiche, dati che rivelano le convenzioni filosofiche o religiose, dati relativi alla salute, dati genetici, dati relativi a condanne penali o reati, dati relativi alla vita/ orientamento sessuale….)

CATEGORIE DI DESTINATARI

Indicare le categorie di soggetti a cui i dati sono comunicati (es. Enti previdenziali, Ministeri …) e gli eventuali responsabili esterni del trattamento e sub-responsabili

TRASFERIMENTO DATI VERSO PAESI TERZI E ORGANIZZAZIONI INTERNAZIONALI

Indicare il Paese terzo o l'organizzazione internazionale a cui i dati sono trasferiti e le garanzie adottate ai sensi del capo V del RGPD

TERMINI ULTIMI DI CANCELLAZIONE PREVISTI

Indicare i tempi di cancellazione previsti. Ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri quali . norme di legge, prassi settoriali indicativi degli stessi (es." in caso di contenzioso, i dati saranno cancellati al termine dello stesso")

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1 . Misure organizzative

a. autorizzazione formale al trattamento

b. istruzioni per il trattamento

c. locali chiusi a chiave in assenza dell'incaricato

d. archivi/ contenitori chiusi a chiave in assenza dell'incaricato

e. accessi controllato al di fuori degli orari di apertura

f. accessi videosorvegliati

g. formazione

h. nomina per iscritto del responsabile esterno

i. altro (indicare)

2. Misure tecniche

a. procedura di autenticazione

b. procedura di autorizzazione

c. procedura di modifica credenziali

d. profilazione

e. salva schermo

f. firewall

g. antivirus

h. disaster recovery

i. antivirus

l. intrusion detection

m. vulnerability assesment/ penetration test

n. cifratura dei dati

o. separazione dei dati

p. adozione delle misure minime di sicurezza ICT

q. altro (indicare)

ALLEGATO B

Dott. ….....

Ufficio / Servizio ….....

Oggetto: Designazione responsabile del trattamento di dati personali

IL DIRIGENTE

Richiamati:

- Il Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27/4/2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»*;

- il Dlgs. 30/6/2003 n.196 e successive modifiche ed integrazioni;

- la disposizione del Sindaco del ..... prot. n. …..... con la quale il sottoscritto è stato nominato titolare delle banche dati e del trattamento dei dati personali del settore …..;

- il Regolamento per l'accesso agli atti, ai documenti ed alle informazioni e per la tutela dei dati personali, approvato con deliberazione del Consiglio Comunale n.157 del 4/7/1994, e successive modifiche e integrazioni;

- il Documento in materia di misure di sicurezza approvato con la deliberazione della Giunta Comunale n..... del …..;

- il Regolamento per il trattamento dei dati sensibili e giudiziari approvato con deliberazione della Giunta Comunale n.763 del 29/11/2005 e successive modifiche e integrazioni;

- la propria determinazione n. …..... avente per oggetto: *"Applicazione delle disposizioni*

in materia di protezione dei dati personali per il Settore .....";

Ritenuto che il dott. …....., responsabile dell'Ufficio/ Servizio …..... , per esperienza, capacità e affidabilità, offra garanzie adeguate a garantire il rispetto della normativa vigente in materia di riservatezza e la tutela degli interessati;

Visto il D.lgs. 267/2000;

Designa

il dott. …..... Responsabile del trattamento dei dati personali e delle banche dati del proprio Ufficio/ Servizio per il periodo di conferimento dell'incarico.

In tale qualità il Responsabile del trattamento è tenuto al rispetto delle disposizioni di legge e di regolamento in materia di tutela dei dati personali osservando i principi di liceità, correttezza. e trasparenza;

In particolare:

- ad adempiere a quanto disposto dal Titolare,
- a organizzare e coordinare l'attività degli incaricati e vigilare che essi operino nel rispetto della legge, nonché dei regolamenti, delle disposizioni, delle procedure e delle istruzioni impartite in materia di protezione dei dati personali;
- a procedere, d'intesa con il Titolare, alla nomina dei soggetti autorizzati al trattamento;
- a verificare che siano rilasciate le informative;
- a controllare che siano osservate le misure tecniche e organizzative di sicurezza adottate dall'Ente;
- a verificare che siano osservate le disposizioni relative all'esercizio dei diritti dell'interessato;
- per quanto di competenza, a riferire tempestivamente al Titolare, le condizioni o le problematiche che siano suscettibili di rendere difficile o pregiudicare la gestione o l'espletamento delle attività nel rispetto della legge e delle disposizioni del sistema di protezione dei dati personali ed, in particolare, qualsiasi elemento oggettivo o soggettivo che abbia compromesso o possa compromettere la sicurezza, la correttezza e la legittimità dei trattamenti anche in ambito informatico;

- a fornire agli incaricati ogni chiarimento necessario o utile alla migliore attuazione e/o gestione del sistema di protezione dei dati personali;
- a riferire tempestivamente al Titolare eventuali violazioni della legge e/o del sistema di protezione dei dati personali di cui viene a conoscenza;
- a interagire con il Responsabile per la protezione dei dati, laddove richiesto, dandone informazione al Titolare.

Delega

il dott. ….....

- a richiedere al preposto alla gestione delle credenziali l'assegnazione e la revoca delle credenziali di autenticazione degli incaricati al trattamento dei dati;

- a richiedere al preposto alla gestione delle credenziali l'accesso alle applicazioni e alle banche dati nonché la modifica e la revoca delle predette autorizzazioni;

- a attivare la procedura prevista per accedere a dati e informazioni contenute nel pc di un proprio operatore, qualora, in caso di assenza o impedimento di quest'ultimo, per esclusiva necessità di operatività o sicurezza, si renda indispensabile e indifferibile intervenire sul pc del lavoratore stesso.

Il Dirigente del Settore

Dott.....

….....

Per ricevuta .....

Data ….....

ALLEGATO C

Spett.le

OGGETTO: Nomina responsabile esterno del trattamento dati ai sensi art. 28 Regolamento EU 679/2016.

Contratto di ….....

1) La ditta …..... (di seguito “Responsabile”) è nominata Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 (nel seguito “Regolamento UE”), per tutta la durata del contratto in oggetto. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del contratto, nei limiti delle finalità' ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE (nel seguito “Normativa in tema di trattamento dei dati personali”) e delle istruzioni nel seguito fornite;

2) Il Responsabile presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali;

3) La finalità del trattamento è l'esecuzione del contratto tra le parti per le attività specificate in oggetto;

4) Le categorie di dati personali trattati sono quelli indicati nel contratto in oggetto con tutte le specifiche ivi contenute;

5) Le categorie di interessati sono …..... *(es. utenti, dipendenti, cittadini .....)*;

6) Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

c) trattare i dati conformemente alle istruzioni scritte del Titolare che il Responsabile si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione della Normativa in tema di trattamento dei dati personali, il Responsabile deve informare immediatamente il Titolare del trattamento;

d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:

   - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
   - ricevano la formazione necessaria in materia di protezione dei dati personali;
   - trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti previsti dalla Normativa in tema di trattamento dei dati personali anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nell'eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE.

7) Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE.

8) Il Responsabile del trattamento può ricorrere a sub-Responsabili del trattamento per gestire attività di trattamento specifiche, informando di ogni nuova nomina e/o sostituzione dei sub- Responsabili il Titolare .

9) I sub-Responsabili del trattamento devono rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportati in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità, risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; il Titolare potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi.

10) Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termine di danno reputazionale) in relazione anche ad una sola violazione della Normativa in materia di trattamento dei dati personali comunque derivata dalla condotta (attiva e/o omissiva) sua o dei sub-Responsabili.

11) Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato

riscontro agli interessati nei termini prescritti.

12) Il Responsabile del trattamento informa il Titolare tempestivamente e, in ogni caso senza ingiustificato ritardo, dell'avvenuta conoscenza, di ogni violazione di dati personali (cd. Data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quando il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile del trattamento o di suoi sub-Responsabili;

13) Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto;

14) Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare – anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione – verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso;

15) Il Responsabile si impegna, su scelta del Titolare, a cancellare o a restituire tutti i dati personali del Titolare dopo che è terminata la prestazione dei servizi relativi al trattamento, salvo che la normativa vigente non ne preveda la conservazione;

16) Il Responsabile si impegna ad attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante “Misure e accorgimenti prescritti ai titolari del trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema” e a comunicare al Titolare i nominativi degli amministratori di sistema;

17) In via generale, il Responsabile del trattamento si impegna ad operare adottando tutte le

misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento eseguito dal Responsabile, o da un sub-Responsabile;

18) Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione stretta da parte del Titolare;

19) Il Responsabile si impegna a non duplicare dati e programmi a cui è consentito l'accesso e a non creare autonome banche dati per finalità diverse da quelle contemplate nel contratto e a garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi di dati, notizie e informazioni circa atti o fatti di cui si è venuti a conoscenza a causa o nell'esercizio della prestazione contrattuale;

20) Nel caso in cui l'oggetto del contratto comporti l'utilizzazione di applicazioni informatiche o banche dati del Comune, per ottenere le relative autorizzazioni all'accesso, il Responsabile dovrà fornire al Responsabile dei Sistemi Informativi, all'inizio della collaborazione, l'elenco delle persone autorizzate al trattamento dei dati per le quali si richiede il rilascio delle credenziali. Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità pari alla durata del contratto, se conosciuta. In caso contrario il periodo di validità delle credenziali è di dodici mesi. Almeno 60 giorni prima della scadenza il preposto alla gestione delle credenziali comunica al Titolare tramite e.mail che, scaduto il periodo di validità, le credenziali dell'utente, salvo diversa comunicazione, saranno disabilitate. Trascorsi 30 giorni dalla scadenza del periodo di validità delle credenziali, senza che sia pervenuta una diversa comunicazione da parte del Dirigente di Settore, l'utente verrà cancellato.

Il Titolare del Trattamento

Firma_____

Il Responsabile del Trattamento

Firma_____

Data _____

ALLEGATO D

Sig.....

Settore ….....

Ufficio ….....

Oggetto: Autorizzazione al trattamento di dati personali

I sottoscritti, per quanto di competenza ai sensi della determinazione n. …..... avente per oggetto: .....

Richiamati:

- l'art.2 quaterdecies del Dlgs.196/2003 - Codice in materia di protezione dei dati personali - e successive modifiche e integrazioni;
- il Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27/4/2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»*;
- la disposizione del Sindaco PG …..... del …....., con la quale il dirigente del Settore …..... è stato nominato titolare delle banche dati e del trattamento dei dati personali ;
- l'art.15 del Regolamento comunale per l'accesso agli atti, ai documenti e alle informazioni e per la tutela dei dati personali, approvato con deliberazione del Consiglio Comunale n.157 del 4/7/1994, modificato ed integrato con deliberazioni del Consiglio Comunale nn.4 e 97 del 1999 e n.68 del 30.10.2006 che prevede che i responsabili del trattamento procedano, d'intesa con il titolare, all'individuazione degli incaricati, cioè delle persone autorizzate nei vari uffici a compiere le operazioni di trattamento dei dati;
- il Regolamento per il trattamento dei dati sensibili e giudiziari approvato con deliberazione della Giunta Comunale n.763 del 29/11/2005 e successive modifiche ed integrazioni;
- il Documento in materia di misure di sicurezza approvato con la deliberazione della Giunta Comunale n.707 del 22/12/2015;
- la determinazione del dirigente del Settore …..n..... avente per oggetto: *"....."*
- la disposizione del dirigente del Settore …..... PG …..di nomina del sig.

…..... quale responsabile del trattamento e delle banche dati dell'Ufficio/ Servizio …..

autorizzano

il sig.....alle operazioni di trattamento di competenza dell'Ufficio....., così come indicate nella scheda allegata alle determinazioni n. …..... sopra citata.

A tal fine impartiscono le seguenti istruzioni:

- I dati possono essere trattati esclusivamente per gli scopi definiti dall'ambito di trattamento indicato nella determinazione sopra citata e non possono in alcun modo essere comunicati a terzi non incaricati.
- Devono essere osservate 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.
- A tale fine deve essere assicurata la custodia e la riservatezza dei dispositivi di autenticazione per il trattamento con l'ausilio di strumenti elettronici, e non deve essere lasciato incustodito e accessibile lo strumento elettronico durante una seduta di trattamento, anche in caso di assenza temporanea dall'ufficio (es. pausa caffè) in particolare negli orari di accesso agli uffici da parte del pubblico esterno. In questo caso bisogna accertarsi che il PC sia spento o disconnesso o, in alternativa, oscurato con modalità salvaschermo (cd. screen-saver) dotata di password.
- 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.
- Si deve evitare di effettuare il trattamento dei dati personali in presenza di terzi che possano così venire a conoscenza, anche occasionalmente, dei dati.

Il Dirigente

del Settore …..

Dott.....

Il Responsabile dell'ufficio/ servizio.....

Dott. …..