PRIVACY

MANUALE OPERATIVO

INDICE

4) TRASFERIMENTO DI UN DIPENDENTE NELL'AMBITO DELLO STESSO SETTORE

- Incarico al trattamento dei dati
- Accesso a nuove applicazioni e banche dati
- Accesso ad applicazioni e banche dati di altro Settore
- Ulteriori adempimenti

5) CESSAZIONE DEL RAPPORTO DI LAVORO

- Revoca dell'accesso ad applicazioni e banche dati;
- Dipendenti a tempo determinato e indeterminato;
- Prestazione occasionale, tirocinio formativo, incarico professionale;
- Ulteriori adempimenti.

6) INTERVENTI DI MANUTENZIONE SULLA POSTAZIONE DI LAVORO

7) ACCESSO ALLA POSTAZIONE DI LAVORO IN CASO DI ASSENZA DEL LAVORATORE

8) PRESCRIZIONI PER IL CORRETTO USO DEGLI STRUMENTI DI LAVORO

- Criteri generali di utilizzo;
- Utilizzo degli strumenti informatici;
- Utilizzo della Rete Internet;
- Utilizzo della posta elettronica;
- Utilizzo degli strumenti di telefonia fissa e mobile;

9) ISTRUZIONI PER LA SICUREZZA E LA PROTEZIONE DEI DATI PERSONALI

- Password:
    - Password collegata ai sistemi centralizzati di autenticazione/ autorizzazione;
    - Cosa fare se la password è scaduta;
    - Cosa fare se si dimentica la password d'accesso al PC;
    - Cosa fare se le credenziali sono disattivate;
    - Password di accesso alle applicazioni informatiche;
    - Cosa fare se si dimentica la password;
- Salvataggio dati**;**
- Antivirus;
- Obbligo di riservatezza. Protezione degli strumenti di lavoro.

10) CONTRATTI / CONVENZIONI CON SOGGETTI ESTERNI *(* ditte, cooperative, professionisti, soggetti pubblici, gestori di pubblici servizi.....)

- Nomina del Responsabile esterno del trattamento dei dati;
- Nomina dell'Amministratore di sistema esterno;
- Accesso ad applicazioni e banche dati del Settore contraente;
- Accesso ad applicazioni e banche dati di altri settori;
- Scadenza credenziali;
- Ulteriori adempimenti.

ALLEGATI

ALLEGATO 1:

- **Nomina del Responsabile Interno del trattamento**

ALLEGATO 2:

- **Nomina incaricato al trattamento** (per accedere a dati e applicazioni del proprio settore)

ALLEGATO 3:

- **Nomina incaricato al trattamento** (per accedere a dati e applicazioni di un settore diverso da quello di appartenenza)

ALLEGATO 4:

- **Nomina del Responsabile Esterno** (convenzioni/ contratti con soggetti pubblici o privati che accedono a banche dati e applicazioni del Comune)

ALLEGATO 5:

- **Informativa**

ALLEGATO 6

- **Segnalazione evento anomalo**

DISPOSIZIONI DI RIFERIMENTO

- Regolamento UE 2016/679 (GDPR);
- Dlgs. 30.6.2003 n. 196 e ss.mm (Codice in materia di protezione dei dati personali)
- Regolamento Comunale per l'accesso agli atti, ai documenti, e alle informazioni e per la tutela dei dati personali;
- Documento sulla sicurezza dei dati personali;
- Regolamento Comunale per il trattamento dei dati sensibili e giudiziari;
- Determinazioni dirigenziali in materia di privacy;
- Disciplinare per l'uso degli strumenti di lavoro e per la registrazione delle presenze e degli accessi;

I Regolamenti, il Documento sulla sicurezza dei dati personali e le determinazioni dirigenziali sono consultabili su COMNET (http:// intranet.comune.modena.it) alla pagina Privacy.

Il Disciplinare per l'uso degli strumenti di lavoro e per la registrazione delle presenze e degli accessi è consultabile su Comnet, nella sezione "Lavorare in Comune" alla pagina "Codice disciplinare " utilizzando il seguente link: https://www.comune.modena.it/amministrazione-trasparente/disposizioni-generali/atti-generali/codice-disciplinare-di-dipendenti-e-dirigenti

1. DEFINIZIONI

- **DATO PERSONALE**

E' qualunque informazione relativa a una persona fisica identificata o identificabile.

Per “identificabile” si intende la persona che può essere identificata direttamente o indirettamente attraverso un identificativo come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economico - culturale o sociale. E' dato personale anche il solo nome o cognome, un numero di matricola, l'immagine di una persona all'interno di un video ecc..

- **CATEGORIE PARTICOLARI DI DATI PERSONALI**

Sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale o all'orientamento sessuale e i dati biometrici intesi ad identificare in modo univoco una persona fisica

- **DATI PERSONALI RELATIVI A CONDANNE PENALI E A REATI O A MISURE DI SICUREZZA CONNESSE**

E' dato personale relativo a condanne penali e reati o a misure di sicurezza connesse il dato idoneo a rivelare una serie di provvedimenti di natura penale; è dato giudiziario quello contenuto nel casellario giudiziale e nell'anagrafe delle sanzioni amministrative dipendenti da reato o quello idoneo a rivelare la qualità di indagato o imputato. Non contiene dati giudiziari il casellario giudiziale che riporta la dicitura “Nulla“ o che riporti unicamente il provvedimento della dichiarazione di fallimento.

- **TRATTAMENTO DEI DATI PERSONALI**

E' qualunque operazione o insieme di operazioni, con o senza l'ausilio di processi automatizzati, riferiti a dati personali o a complessi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la consultazione, l'uso, l'elaborazione, la modificazione, l'estrazione, l'utilizzo, la comunicazione mediante trasmissione, la diffusione o qualsiasi forma di messa a disposizione, il raffronto, l'interconnessione, la limitazione, la cancellazione e la distruzione

- **TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI**

Titolare del trattamento è il Comune di Modena. L'esercizio delle relative competenze è

attribuito dal Sindaco, con proprio provvedimento, al Dirigente della struttura, di norma titolare di PEG.
Al Titolare competono le decisioni in ordine alle finalità, alle modalità di trattamento dei dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza. Al Titolare è attribuito il compito di mettere in atto politiche adeguate in materia di protezione dei dati, adottando il registro dei trattamenti ed eventuali misure tecniche e organizzative aggiuntive rispetto a quelle contenute nel Documento sulla sicurezza dei dati personali, atte a garantire che il trattamento sia effettuato conformemente al GDPR.
I Dirigenti titolari di PEG, sulla base delle disposizioni contenute nel Regolamento Comunale per l'accesso agli atti, ai documenti, e alle informazioni e per la tutela dei dati personali, nel Regolamento Comunale per il trattamento dei dati sensibili e giudiziari e nel Documento sulla sicurezza dei dati personali, assumono con propria determinazione le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare in particolare:

- fornisce all'interessato l'informativa di 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 con l'eventuale supporto del Responsabile per la protezione dei dati. Si applicano al riguardo, laddove non diversamente normato, le disposizioni e i termini di cui al Regolamento Comunale sull'attività e sui procedimenti amministrativi
- nel caso in cui un tipo di trattamento 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, secondo lo schema (**Allegato 1**) dei Dirigenti, dei Responsabili, dei Funzionari e degli Incaricati di Elevata qualificazione 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;
- 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 4**);
- provvede, attraverso il Responsabile per la protezione dei dati e con le modalità previste dal Manuale per la gestione di una violazione dei dati personali (

https://www.comune.modena.it/amministrazione-trasparente/disposizioni-generali/atti-generali-1/gestione-violazione-di-dati-personali-data-breach)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;

- cura la formazione dei propri dipendenti avvalendosi, se lo ritiene opportuno, della collaborazione dell'ufficio che si occupa dell'organizzazione dell'attività formativa;
- 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, così come previsto dall'art. 26 del RGPD, 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.

- **RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI PERSONALI**

Responsabile interno del trattamento è il Dirigente di servizio, il Funzionario o l'incaricato di Elevata qualificazione delle singole strutture in cui si articola il settore.
E' nominato dal Titolare del trattamento, sulla base dei necessari requisiti di esperienza, capacità e affidabilità, utilizzando l'apposito modello **(Allegato 1).**
La nomina del Responsabile interno del trattamento è facoltativa: nel caso non venga designato il Titolare è responsabile di tutte le operazioni di trattamento.
Se esigenze organizzative lo rendono necessario, possono essere nominati anche più Responsabili interni per il trattamento dei medesimi dati. In caso di assenza o di impedimento del Responsabile può essere nominato un sostituto.
Il Responsabile procede, tra l'altro, d'intesa con il Titolare, se richiesto, alla nomina dei soggetti autorizzati al trattamento, organizza e coordina l'attività degli incaricati, vigilando sul fatto che operino nel rispetto della normativa in materia di privacy e delle istruzioni ricevute, verifica che siano rilasciate le informative, controlla che siano osservate le misure tecniche e organizzative di sicurezza adottate dall'Ente e verifica che siano osservate le disposizioni relative all'esercizio dei diritti dell'interessato.

Il Responsabile è tenuto altresì a:

• riferire tempestivamente al Titolare, per quanto di propria competenza, i fatti che possono incidere sul legittimo e regolare svolgimento delle attività di trattamento 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 con le modalità previste dal Manuale per la gestione di una violazione dei dati personali (https://www.comune.modena.it/amministrazione-trasparente/disposizioni-generali/atti-generali-1/gestione-violazione-di-dati-personali-data-breach) ;

• garantire un rapporto di permanente e leale collaborazione con il Responsabile per la protezione dei dati dandone informazione , ove necessario, al Titolare .

Il Dirigente di settore può altresì delegare il Responsabile a chiedere, revocare, modificare le autorizzazioni del lavoratore ad accedere alle banche dati e alle applicazioni.

- **INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI**

Si definisce "incaricato" qualsiasi dipendente che, nello svolgimento delle proprie mansioni ha accesso a dati personali e, pertanto, viene appositamente autorizzato; diversamente nessun dipendente può trattare dati personali.

L'incarico viene attribuito dal Titolare del trattamento assieme al Responsabile interno del trattamento, se richiesto, per iscritto e utilizzando l'apposito modello **(Allegato 2).**
Nell'incarico devono essere individuate le tipologie di trattamento che si è autorizzati a compiere.
Ogni soggetto autorizzato al trattamento è tenuto ad effettuare esclusivamente le operazioni e i trattamenti individuati nel predetto incarico, attenendosi alle istruzioni ricevute, e non può procedere ad operazioni e/o trattamenti diversi senza una nuova autorizzazione−al trattamento, sempre in forma scritta.

Ciascun incaricato è tenuto, in particolare:

• a eseguire o applicare le disposizioni impartite;

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

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 informatici, e non deve essere lasciato incustodito e accessibile lo strumento informatico 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.

Per quanto riguarda invece i trattamenti senza strumenti informatici, 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.

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

• segnalare tempestivamente all'indirizzo e-mail responsabileprotezionedati@comune.modena.it eventuali eventi anomali che possono determinare la violazione di dati personali, utilizzando l'apposito modello secondo lo schema (**Allegato 6**)

- **CREDENZIALI DI AUTENTICAZIONE**

Sono:

1) user - id (codice di autenticazione), d'ora innanzi “user - id”;

2) password (parola chiave), d'ora innanzi “password”.

Entrambe sono necessarie per poter utilizzare la strumentazione informatica e telematica. Nel rispetto di quanto richiesto dalle Misure Minime di sicurezza ICT per la Pubbliche Amministrazioni di cui all'art.1 del presente Documento sulla sicurezza dei dati personali, le credenziali sono nominative e riconducibili ad una sola persona.

- **PREPOSTO ALLA GESTIONE DELLE CREDENZIALI PER L'ACCESSO ALLE BANCHE DATI CENTRALIZZATE CHE UTILIZZANO I SISTEMI LDAP E ACTIVE DIRECTORY**

E' il Responsabile dell'Ufficio Reti e Sistemi del settore a cui compete la gestione del sistema informatico/telematico del Comune; esso svolge la funzione di assegnare/ revocare le credenziali di autenticazione e di abilitare all'accesso a banche dati ed applicazioni.
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.

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.

La password è provvisoria e dovrà essere immediatamente sostituita da una a lui conosciuta.

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.

RESPONSABILI INFORMATICI DELLE APPLICAZIONI

Sono gli operatori tecnici del che si occupano della gestione informatica delle applicazioni e delle banche dati dei settori.

- **AMMINISTRATORI DI SISTEMA**

Sono Amministratori di sistema gli operatori tecnici del Settore a cui compete la gestione

del sistema informatico / telematico o di società esterne che si occupano della installazione, gestione e manutenzione di un sistema di elaborazione o di sue componenti, delle reti e degli apparati di sicurezza, dei data base, dei sistemi software complessi.

Il Dirigente del Settore a cui compete la gestione del sistema informatico / telematico nomina i dipendenti del proprio settore incaricati a svolgere le attività di Amministratore di Sistema, nel rispetto del Provvedimento del Garante per la protezione dei dati personali n. 300 del 24 dicembre 2008, così modificato dal Provvedimento n. 149 del 30 giugno 2009.

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.

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.

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**.**

2. COSTITUZIONE DI UN NUOVO RAPPORTO DI LAVORO

- **INCARICO AL TRATTAMENTO DEI DATI**

Ogni lavoratore che tratta dati personali deve essere incaricato del trattamento dei dati utilizzando l'apposito modello **(Allegato 2).** L'incarico è dato congiuntamente dal titolare (Dirigente del Settore) e dal Responsabile interno del trattamento dei dati, se richiesto.

- **ASSEGNAZIONE DELLA CASELLA DI POSTA ELETTRONICA E ACCESSO A INTERNET**

Per avere una casella di posta elettronica e accedere a Internet il lavoratore deve possedere le credenziali di autenticazione costituite da user- id e password.
Tali credenziali devono essere richieste dal Dirigente del settore di competenza/ Responsabile delegato al preposto alla gestione delle credenziali attraverso l'apposita

procedura informatica , accedendo da Profilo utente – Abilitazioni.
Per motivi di sicurezza la password assegnata dal preposto alla gestione delle credenziali viene comunicata in maniera riservata al dipendente, è provvisoria e dovrà essere immediatamente sostituita dal lavoratore con una conosciuta solo da lui.
Il lavoratore può in qualsiasi momento cambiare tale password accedendo al sito https://password.comune.modena.it/_dove potrà scegliere la nuova password tra quelle proposte dal sistema.

- **PASSWORD DI ACCESSO AL PC**

Su ogni computer è impostato un profilo per l'accesso al PC con user-id e password provvisoria .
Il lavoratore deve immediatamente sostituire la password provvisoria nel rispetto della normativa vigente.
Per motivazioni tecniche la nuova password è uguale a quella per l'accesso ad internet e per la posta elettronica.

- **ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE**

Ad ogni singolo operatore possono essere assegnate più credenziali di autenticazione , diverse fra loro, a seconda dei sistemi e delle procedure applicative a cui accede (banche dati, cartelle condivise ....)

- **ACCESSO AD APPLICAZIONI E BANCHE DATI DEL PROPRIO SETTORE**

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

L’autorizzazione del singolo lavoratore ad accedere alle banche dati del Comune deve essere sempre preceduta dal conferimento dell’incarico al trattamento dei dati da parte del Responsabile del trattamento dei dati d'intesa con il Titolare del trattamento.

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.

Il Dirigente del Settore di appartenenza/Responsabile 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 ALTRO SETTORE**

Il Dirigente/Responsabile del settore a cui il lavoratore appartiene inoltra la richiesta per iscritto, anche via e- mail, al Dirigente del settore titolare della banca dati, ~~da utilizzare~~ specificando il nominativo del lavoratore e le abilitazioni richieste.
Il Dirigente titolare della banca dati predispone l'incarico al trattamento dei dati per il lavoratore utilizzando l'apposito modello **(Allegato 3)** che viene sottoscritto congiuntamente dal Dirigente del settore a cui il lavoratore appartiene e dal Dirigente titolare della banca dati.

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.

3.TRASFERIMENTO DI UN DIPENDENTE PRESSO UN ALTRO SETTORE

INCARICO AL TRATTAMENTO DEI DATI

Ogni lavoratore che tratta dati personali deve essere incaricato del trattamento dei dati utilizzando l'apposito modello **(Allegato 2).** L'incarico è dato congiuntamente dal titolare (dirigente del settore in cui il dipendente si è trasferito) e dal responsabile interno del trattamento dei dati

ACCESSO A NUOVE APPLICAZIONI E BANCHE DATI

Il preposto alla gestione delle credenziali, dopo avere rilevato l'informazione attraverso la banca dati centralizzata del Settore che gestisce il personale, revoca tutte le abilitazioni all'accesso, ad eccezione dell'indirizzo di posta elettronica, di cui il dipendente rimane titolare e ne informa, attraverso l'apposita procedura informatica, il responsabile informatico dell'applicazione.

Il dirigente del settore di nuova assegnazione (o il responsabile delegato) provvede a richiedere le nuove abilitazioni con le stesse modalità previste nel caso di costituzione di un nuovo rapporto di lavoro.

ACCESSO AD APPLICAZIONI E BANCHE DATI DI ALTRO SETTORE

Se il lavoratore deve accedere a banche dati di un altro settore, si procede con le stesse modalità previste nel caso di costituzione di un nuovo rapporto di lavoro.

ULTERIORI ADEMPIMENTI

Su richiesta del dirigente di settore, il lavoratore trasferito è tenuto a reindirizzare al settore di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo.
Il lavoratore, nel caso in cui mantenga il proprio PC, è tenuto, prima del trasferimento, a trasmettere al dirigente del settore di provenienza i dati e,su richiesta del dirigente di settore, le e.mail di interesse del settore stesso e successivamente a rimuoverli dalla propria stazione di lavoro.
Se invece non porta con sè il PC, il lavoratore, prima del suo trasferimento, deve eliminare i documenti e le e-mail che non siano di interesse del settore, autorizzando, attraverso l'apposita procedura informatica, il dirigente del settore ad accedere ai documenti ed alle e-mail rimanenti e dichiarando di avere provveduto alla eliminazione dei dati e delle e.mail che non sono di interesse del Settore.
Il dirigente del settore/ responsabile delegato deve prontamente avvisare il responsabile dell'Ufficio Reti e Sistemi (preposto alla pulizia e recupero delle banche dati) concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti

4. TRASFERIMENTO DI UN DIPENDENTE NELL'AMBITO DELLO STESSO SETTORE

INCARICO AL TRATTAMENTO DEI DATI

Se il lavoratore, a seguito del trasferimento, tratta dati personali diversi da quelli trattati in precedenza deve essere nuovamente incaricato del trattamento dei dati utilizzando l'apposito modello **(Allegato 2)**
L'incarico è dato congiuntamente dal titolare (Dirigente del Settore di appartenenza) e dal responsabile del trattamento dei dati

ACCESSO A NUOVE APPLICAZIONI E BANCHE DATI

Il dirigente di settore/ responsabile delegato, sulla base delle nuove competenze attribuite al dipendente, comunica al preposto alla gestione delle credenziali attraverso l'apposita procedura informatica , accedendo da Profilo utente - Abilitazioni le autorizzazioni all'accesso da revocare e le nuove applicazioni alle quali il lavoratore è autorizzato ad accedere.
Il preposto alla gestione delle credenziali ottempera alle richieste e , attraverso la medesima procedura informatica, ne informa il dirigente di settore ed il responsabile informatico dell'applicazione.

ACCESSO AD APPLICAZIONI E BANCHE DATI DI ALTRO SETTORE

Se il lavoratore deve accedere a banche dati di un altro settore, si procede con le stesse modalità previste nel caso di costituzione di un nuovo rapporto di lavoro.

ULTERIORI ADEMPIMENTI

Su richiesta del dirigente di settore, il lavoratore trasferito è tenuto a reindirizzare all'ufficio di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo.
Il lavoratore, nel caso in cui mantenga il proprio PC, è tenuto, prima del trasferimento, a trasmettere al dirigente del settore di provenienza i dati e, su richiesta del dirigente di settore, le e.mail di interesse del settore stesso e a rimuovere i dati dalla propria stazione di lavoro. Se invece non porta con sè il PC, il lavoratore, prima del suo trasferimento, deve eliminare dalla sua stazione di lavoro i documenti e le e-mail che non siano di interesse del settore, autorizzando , attarverso l'apposita procedura informatica, il dirigente ad accedere ai documenti ed alle e-mail rimanenti dichiarando di avere provveduto alla eliminazione dei dati e delle e.mail che non sono di interesse del Settore
Il dirigente del settore/ responsabile delegato deve prontamente avvisare il responsabile dell'Ufficio Reti e Sistemi(preposto alla pulizia e recupero delle banche dati) concordando con lui le modalità di gestione della stazione di lavoro e dei dati in essa contenuti

5.CESSAZIONE DEL RAPPORTO DI LAVORO

- **REVOCA DELL'ACCESSO AD APPLICAZIONI E BANCHE DATI**

Dipendenti a tempo indeterminato o determinato

Dopo 90 giorni dalla data di cessazione del rapporto di lavoro il preposto alla gestione delle credenziali ricava, attraverso una procedura automatica, 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.

Prestazione occasionale, tirocinio formativo, incarico professionale

Il Dirigente del settore competente/ responsabile delegato comunica tempestivamente al preposto alla gestione delle credenziali, attraverso l'apposita procedura informatica, accedendo da Profilo utente - Abilitazioni, la cessazione del rapporto di lavoro e chiede 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 il dirigente di settore ed il responsabile informatico dell'applicazione.

- **ULTERIORI ADEMPIMENTI**

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 del settore ad accedere ai documenti ed alle e-mail rimanenti**.**
Il Dirigente del Settore/Responsabile delegato deve prontamente avvisare il Responsabile dell'Ufficio Reti e Sistemi (preposto alla pulizia e recupero delle banche dati), 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 e autorizza l'intervento del tecnico dell'Ufficio Reti e Sistemi che avverrà, laddove possibile, alla presenza dell'interessato.

Questo intervento deve essere 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 si provveda al ritiro della stazione di lavoro, i dati legati al profilo del lavoratore verranno resi indisponibili dopo averne trattenuto una copia. Il Dirigente del settore/ responsabile delegato ha tempo un mese per chiedere il recupero di eventuali 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 a 6 mesi dalla cessazione del dipendente, così come la *home directory.*

6. INTERVENTI DI MANUTENZIONE SULLA POSTAZIONE DI LAVORO

Il lavoratore deve concordare modi e tempi di intervento con i tecnici addetti.
Se per un intervento di manutenzione è necessario accedere al PC utilizzando le credenziali del lavoratore, queste, non vanno comunicate al tecnico ma devono essere inserite dal lavoratore stesso.

Nel caso in cui il lavoratore non possa presenziare all'intervento, verrà creata una password provvisoria per il solo accesso al pc da parte del tecnico, dopodichè, alla riconsegna, l'utente dovrà cambiare la password di lavoro.

7. ACCESSO ALLA POSTAZIONE DI LAVORO IN CASO DI ASSENZA DEL LAVORATORE

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 interno 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 lavoratore può individuare un collega che assista alle operazioni di accesso a dati, procedure e e.mail del proprio pc da parte del Dirigente/ responsabile delegato. Il Dirigente Responsabile di Settore/ il responsabile delegato richiede ed autorizza l'intervento dei tecnici dell'Ufficio Reti e Sistemi, che permettono l'accesso al pc per il tempo necessario.

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

Nel caso in cui non sia stato individuato alcun lavoratore oppure nel caso in cui anche il lavoratore individuato non sia presente, le suddette operazioni verranno svolte alla presenza di un altro collega, individuato dal Dirigente / Responsabile delegato.

Gli interventi dei tecnici dell'Ufficio Reti e Sistemi 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.

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.

8. PRESCRIZIONI PER IL CORRETTO USO DEGLI STRUMENTI DI LAVORO

- **CRITERI GENERALI DI UTILIZZO**

Le norme di comportamento per un corretto uso degli strumenti informatici, della rete informatica e telematica e del sistema di telefonia fissa e mobile sono contenute all'interno del Disciplinare per l'uso degli strumenti di lavoro e per la registrazione delle presenze e degli accessi e nel Codice di Comportamento del Comune di Modena.
Il mancato rispetto delle regole e dei divieti in essi elencati, oltre a comportare eventuali responsabilità sotto i profili amministrativo, civile e penale, costituisce, per i dipendenti violazione del Codice di Comportamento e, per i collaboratori esterni, violazione degli obblighi contrattuali.
Gli strumenti informatici (a titolo esemplificativo e non esaustivo personal computer, stampante), telematici (a titolo esemplificativo e non esaustivo accesso ad internet, tramite collegamento fisso o mobile, la posta elettronica), telefonici (a titolo esemplificativo e non esaustivo telefono fisso, cellulare) messi a disposizione degli utenti, costituiscono strumenti

di lavoro.
Pertanto, l'utilizzo di essi da parte degli utenti è consentito per finalità attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta e nel rispetto delle disposizioni normative ed interne e delle esigenze di funzionalità e di sicurezza dei sistemi informativi. Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate alla stessa, quali ad esempio quelle che attengono allo svolgimento del rapporto di lavoro. Va evitato qualsivoglia uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga in modo non ripetuto o per periodi prolungati. E' consentito l'utilizzo degli strumenti informatici del Comune per poter assolvere a incombenze personali senza allontanarsi dalla sede di servizio, a condizione che ciò avvenga al di fuori dell'orario di lavoro.
Per tale utilizzo il Comune è esonerato da ogni responsabilità amministrativa, civile e penale.
L'utilizzo di tali strumenti messi a disposizione non configura alcuna titolarità, da parte del lavoratore, dei dati e delle informazioni trattate, che appartengono al Comune ed ai quali il Comune si riserva, pertanto, il diritto di accedere nei limiti consentiti dalle norme di legge e contrattuali. L'utente deve custodire e utilizzare gli strumenti affidatigli in modo appropriato, con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza del sistema.
Particolare attenzione deve essere prestata nel caso in cui la strumentazione sia utilizzata durante l'attività lavorativa a distanza.
Gli strumenti sono configurati in modo da garantire il rispetto delle regole descritte nel Disciplinare e tale configurazione non deve essere mutata.
L'utente è tenuto ad informare direttamente e tempestivamente il proprio Dirigente di settore o il responsabile da questi delegato, nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli strumenti e/o del sistema.

- **UTILIZZO DEGLI STRUMENTI INFORMATICI**

E' vietato:

a) installare sulla stazione di lavoro software, anche se gratuiti (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati dal Comune e collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dal Comune.

b) alterare, disattivare o modificare le impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, della posta elettronica e di ogni altro software installato sulle stazioni di lavoro. Al contrario l'incaricato deve effettuare quanto di competenza per garantirne il funzionamento segnalando tempestivamente al dirigente di settore/responsabile delegato ogni anomalia o disfunzione.

c) accedere al Bios delle stazioni di lavoro e impostare protezioni o password ulteriori rispetto a quelle contemplate nel Documento sulla sicurezza dei dati personali che limitino l'accesso alle stazioni di lavoro stesse.

d) caricare, detenere nelle stazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa.

e) in ogni caso, caricare, detenere e/o stampare materiale informatico:

- il cui contenuto (a mero titolo esemplificativo e non esaustivo : testo, audio, video) sia coperto da diritto d'autore.
Nel caso in cui ciò sia necessario per la propria attività lavorativa, l'utente è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;

- il cui contenuto sia contrario a norme di legge.

f) utilizzare, presso la sede di lavoro, un pc personale o comunque non di proprietà del Comune, collegandolo al sistema, se non espressamente autorizzati.

A titolo esemplificativo, ma non esaustivo, sono considerate modifiche del sistema:

a) modificare i collegamenti di rete esistenti;

b) disattivare o alterare la configurazione dei software di sicurezza (antivirus) ;

c) usare dispositivi removibili (CD, dvd, hard disk, floppy etc.) per alterare la procedura di avvio del dispositivo ed in particolare per effettuare l'avvio di un sistema operativo diverso da quello fornito dal Comune;

d) aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;

e) installare, senza l'assistenza di personale autorizzato, un qualsiasi software, inclusi quelli scaricati da Internet, o comunque alterare la configurazione della stazione di lavoro assegnata.

Le cartelle utenti presenti nei server del Comune sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.
Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in questa unità.
Su tale unità vengono svolte regolari attività di amministrazione e back up da parte del personale incaricato nonché attività di verifica nel caso venga richiesta.

- **UTILIZZO DELLA RETE INTERNET**

L'accesso alla Rete Internet costituisce strumento di lavoro ed è consentito per finalità direttamente attinenti o comunque connesse all'esercizio dell'attività lavorativa.
E' escluso qualsivoglia uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza o di necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.
E' consentito l'accesso per poter assolvere a incombenze personali senza allontanarsi dalla sede di servizio, a condizione che ciò avvenga al di fuori dell'orario di lavoro. Il Comune è esonerato da ogni responsabilità amministrativa, civile e penale al riguardo. L'utente è responsabile altresì di eventuali danni all'integrità e disponibilità del sistema eventualmente causati da tale utilizzo.
E' **vietato** entrare nella rete e nei programmi con un codice di identificazione diverso da quello assegnato. Le password di ingresso alla rete ed ai programmi sono segrete e vanno gestite secondo le istruzioni e le procedure impartite (vedi alla voce **Password).**

E', altresì, **vietato**:

- scaricare e/o installare software non espressamente autorizzati dal Comune;
- scaricare e/o usare materiale informatico non direttamente attinente all'esercizio dell'attività lavorativa;
- scaricare e/o usare materiale informatico il cui contenuto (a mero titolo esemplificativo: software, testo, audio e video) sia coperto da diritto di autore. Nei casi in cui ciò sia necessario per lo svolgimento dell'attività lavorativa, il lavoratore è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;
- partecipare a forum di discussione on line, a chat, utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa;
- navigare in internet su siti contrari a norme di legge;
- effettuare ogni genere di transazione finanziaria per fini personali;
- installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia PEER to PEER (es.eMule, kazaa, bittorrent etc.) indipendentemente dal contenuto dei file scambiati;
- usare i profili social del Comune per fini personali, politici o commerciali
- utilizzare i profili personali attivati sui social media per agire in nome e per conto del Comune,
- utilizzare strumenti di filesharing quali, a mero titolo esemplificativo, Dropbox, Google Drive, One Drive, I-Cloud Drive, se non espressamente autorizzati dai Sistemi informativi.

- **UTILIZZO DELLA POSTA ELETTRONICA**

L'utilizzo della posta elettronica è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa.
E' escluso l'uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto.

E' consentito l'utilizzo per poter assolvere a incombenze personali senza allontanarsi dalla sede di servizio, a condizione che ciò avvenga al di fuori dell'orario di lavoro. Per tale utilizzo il Comune è esonerato da ogni responsabilità amministrativa, civile e penale. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dall'incaricato nel rispetto dei criteri e delle regole indicati dal Documento sulla sicurezza dei dati personali. L'accesso alla casella di posta elettronica è reso sicuro dall'utilizzo del protocollo di comunicazione cifrato tramite apposito certificato.

E' **vietato**:

a) inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, ed in ogni caso contrari a norme di legge o idonei a creare danno al Comune o a terzi; nonché messaggi a catena e/o spam;

b) scambiare messaggi impersonando un mittente diverso da quello reale;

c) scambiare messaggi di posta contenenti file o link a siti con contenuti illegali, violenti, o pornografici, file o materiale informatico soggetto al diritto d'autore, password e/o codici d'accesso a programmi soggetti a diritto d'autore e/o a siti internet;

d) aprire messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio;

e) inviare, anche da una casella di posta privata, messaggi di natura personale e non attinenti al rapporto di lavoro a indirizzi di posta elettronica contraddistinti dal dominio “comune.modena.it”;

f) inviare messaggi di natura istituzionale da una casella di posta privata, fatti salvi i casi di forza maggiore dovuti a circostanze per cui l'utente, per qualsiasi ragione, non può accedere alla casella istituzionale. “

In caso di assenze programmate dal lavoro (per ferie o per qualsiasi altro motivo), utilizzando la funzione “Fuori Ufficio” deve essere attivato preventivamente 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 al contenuto delle e-mail del lavoratore assente 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 lavoratore può

individuare un collega che assista alle operazioni di accesso alle e.mail da parte del Dirigente o del responsabile delegato.
Il Dirigente Responsabile di Settore o il responsabile delegato richiede ed autorizza l'intervento dei tecnici dell'Ufficio Reti e Sistemi, che permettono l'accesso al pc per il tempo strettamente necessario.
Di tale attività è redatto apposito verbale a cura del dirigente/responsabile ed è informato l'utente alla prima occasione utile. Nel caso in cui non sia stato nominato alcun lavoratore, oppure nel caso in cui anche il lavoratore individuato non sia presente, le suddette operazioni verranno svolte alla presenza di un altro collega, individuato dal Dirigente / responsabile delegato.
Di tale attività è redatto apposito verbale a cura del dirigente/responsabile ed è informato l'utente alla prima occasione utile.
Il Dirigente di settore, qualora rilevi un utilizzo improprio della posta elettronica da parte di un utente o comunque una violazione delle regole e dei divieti di cui al Disciplinare per l'uso degli strumenti di lavoro e e per la registrazione delle presenze e degli accessi, ne informa l'utente interessato che potrà chiedere di essere ascoltato e di accedere alla relativa documentazione.
A seguito delle verifiche effettuate, il dirigente di settore avvia, se del caso, i procedimenti conseguenti.

- **UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE**

Gli strumenti di telefonia (sia fissa che mobile) messi a disposizione dal Comune costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa.
E' escluso l'uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza e di necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.
E' consentito l'utilizzo per poter assolvere a incombenze personali senza allontanarsi dalla sede di servizio, a condizione che ciò avvenga al di fuori dell'orario di lavoro. Per tale utilizzo il Comune è esonerato da ogni responsabilità amministrativa, civile e penale.
Nelle giornate di lavoro a distanza, il trasferimento delle chiamate dal telefono dell'ufficio alla sede di svolgimento del lavoro a distanza è assicurato in relazione al numero di licenze disponibili e quindi utilizzando dei criteri di priorità dei servizi.

- **UTILIZZO DEGLI STRUMENTI PER LA REGISTRAZIONE DEGLI ACCESSI E DELLE PRESENZE**

Il Comune è dotato di una procedura di registrazione automatica delle presenze e degli accessi che consentono di rilevare la presenza e di registrare l'accesso e/o presenza anche presso altre sedi o locali attraverso apposito badge. Tale procedura consente altresì al dipendente, qualora non abbia provveduto alla timbratura attraverso il badge, di registrare l'entrata e/o l'uscita, previa autorizzazione del proprio dirigente, attraverso il portale del dipendente.
Nelle sedi direzionali del Comune dotate di apri porta, l'accesso fuori dall'orario di lavoro avviene attraverso un badge ed è consentito solo per motivi attinenti l'attività lavorativa e per le finalità con essa attinenti e connesse.

La registrazione delle presenze da parte di dirigenti e dipendenti avviene nel rispetto delle modalità indicate nel Regolamento sull'ordinamento degli uffici e servizi pubblicato sul sito del Comune di Modena.
Il dirigente responsabile di settore in quanto titolare del trattamento dei dati, nonché i responsabili degli uffici/ servizi e, in genere, i soggetti autorizzati dal dirigente, in quanto incaricati del trattamento, accedono ai cartellini dei dipendenti ad essi subordinati e possono effettuare verifiche sugli stessi, con le modalità individuate da ogni singolo settore. Le verifiche possono essere effettuate a campione oppure in modo puntuale qualora vi siano elementi che possono fare pensare ad un uso improprio o non corretto degli strumenti di registrazione delle presenze e degli accessi o che comunque vi sia stata una violazione delle regole e dei divieti in materia di cui al Regolamento sopra richiamato. Qualora le verifiche compiute abbiano esito positivo, il dirigente responsabile avvia i procedimenti conseguenti.
I dati relativi agli accessi vengono conservati, per le finalità sopra indicate, per un periodo di 6 mesi.

9. ISTRUZIONI PER LA SICUREZZA E LA PROTEZIONE DEI DATI PERSONALI

Qualsiasi trattamento dei dati deve avvenire nel rispetto di idonee misure di sicurezza.
Tali misure sono individuate nel Documento sulla sicurezza dei dati personali e nelle determinazioni che ogni Dirigente responsabile di PEG ha assunto in materia.
Il Dirigente/ Responsabile impartisce le istruzioni opportune per ridurre al minimo i rischi di distruzione e perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità perseguite.

- **PASSWORD**

Ogni lavoratore può avere più credenziali di autenticazione, diverse fra loro, a seconda dei sistemi e delle procedure applicative a cui accede (posta elettronica e navigazione Internet, banche dati, cartelle condivise ....).
Le credenziali di autenticazione sono costituite dalla userid (codice di autenticazione corrispondente di norma ad una abbreviazione del proprio nome e cognome) e dalla password (parola chiave) .
Ad ogni lavoratore possono dunque essere assegnate più credenziali di autenticazione. Ogni password deve essere composta da un minimo di dieci caratteri, devono contenere lettere maiuscole e minuscole dell'alfabeto, numeri E caratteri non alfanumerici (quali il punto esclamativo o dollaro o underscore …) non deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere sostituita con scadenza trimestrale.
Per motivazioni tecniche è opportuno avere un'unica password per l'accensione del PC e per l'apertura della posta elettronica.
Le password devono essere custodite con la massima attenzione e segretezza. Fatta eccezione per la procedura prevista per l'accesso al PC del lavoratore assente, le password non devono essere comunicate a terzi né divulgate, né date in risposta a mail che le richiedono. Le password non vanno mai mandate via mail per nessun motivo. Il lavoratore è responsabile di ogni utilizzo indebito o non consentito delle password di cui sia titolare; qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti,

deve prontamente provvedere a modificarla, provvedendo a notificare il cambio all'ufficio Reti e Sistemi.

- Password collegata ai sistemi centralizzati di autenticazione/ autorizzazione (es. accensione PC, posta elettronica e servizi WEB del Comune) (su sistemi di autenticazione LDAP e Active Directory). Le password collegate a sistemi centralizzati di autenticazione/autorizzazione LDAP e Active Directory (quelle che consentono di utilizzare la posta elettronica, di accesso al PC **e servizi WEB del Comune** , di accedere a banche dati centralizzate, a server.....) scadono automaticamente ogni tre mesi. In prossimità della scadenza, l'Ufficio Reti e Sistemi invia un messaggio di posta elettronica al lavoratore interessato che è tenuto a provvedere per tempo alla sostituzione della password con una nuova scelta tra quelle proposte dal sistema. Nel caso in cui il lavoratore non sia dotato di e.mail, l'avviso di scadenza viene mandato tramite SMS, se è stato fornito il numero di cellulare durante la procedura di cambio password.

Cosa fare se la password è scaduta

E' possibile in qualsiasi momento avere una nuova password autenticandosi al sito http://password.comune.modena.it con userid e la vecchia password (valida per questa funzione anche se scaduta) scegliendo la nuova password tra quelle proposte dal sistema

Cosa fare se si dimentica la password di accesso al PC

Il lavoratore dovrà:

- rivolgersi al lavoratore da lui delegato alla custodia della password (vedi alla voce " *Accesso alla postazione di lavoro in caso di assenza del lavoratore")*.

oppure:

- rivolgersi all'Ufficio Reti e Sistemi 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 numero di 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.

Cosa fare se le credenziali sono state disattivate

Le credenziali che non vengono usate per almeno sei mesi continuativi vengono automaticamente disattivate. Per riattivarle il lavoratore dovrà recarsi presso l'Ufficio Reti e Sistemiche provvederà, previa identificazione, a fornire al lavoratore una password provvisoria. Con questa password il lavoratore potrà accedere alla procedura di autenticazione. La password dovrà poi essere immediatamente sostituita da una nuova scelta dal lavoratore.

Oppure, telefonando all'Ufficio Reti e Sistemi, il quale manderà un SMS al numero di cellulare precedentemente comunicato dal lavoratore, con un codice d'accesso con cui ottenere una password provvisoria che consentirà poi di accedere alla procedura di modifica ed ottenere quella definitiva.

- Password di accesso alle applicazioni informatiche (se questa è differente da quella per l'accesso al PC e per l'apertura della posta elettronica).

La password per l'accesso a tutte le applicazioni informatiche che contengono dati personali, deve essere cambiata con cadenza almeno trimestrale, anche nel caso in cui i sistemi non ne prevedano la scadenza automatica.

- **SALVATAGGIO DATI**

L'operazione di salvataggio delle banche dati esistenti sui server, degli archivi documentali e delle banche dati strutturate è in carico all'Ufficio Reti e Sistemi.
E' vietata la creazione di banche dati residenti solo su PC (escludendo pertanto, ad esempio, le banche dati che il lavoratore ha creato ad uso proprio, quelle di cui esiste una copia cartacea ed in genere, quelle che è possibile ricostruire attingendo ad altre banche dati).
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.
Ogni singolo operatore è responsabile del salvataggio degli archivi esistenti sul proprio PC.
E' vietato l'uso di chiavette USB e altri dispositivi mobili per la raccolta e conservazione di dati personali.

- **ANTIVIRUS**

Su tutti i PC 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.

Il software antivirus provvede settimanalmente ad effettuare una scansione completa dei dischi interni della stazione di lavoro una volta a settimana.

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

- **OBBLIGO DI RISERVATEZZA. PROTEZIONE DEGLI STRUMENTI DI LAVORO**

Va mantenuta l'assoluta riservatezza sulle informazioni di cui si viene a conoscenza nel corso delle operazioni del trattamento.
Possono essere trattati esclusivamente i dati necessari per gli scopi definiti dall'ambito di trattamento indicato nella determinazione assunta dal Dirigente in materia di misure di

sicurezza e non possono in alcun modo essere comunicati a terzi non incaricati.
I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
Occorre assicurare l'esattezza, la disponibilità, l'integrità e il tempestivo aggiornamento dei dati trattati., verificandone altresì pertinenza, completezza e non eccedenza rispetto agli scopi per cui sono stati raccolti e successivamente trattati.
I dati personali devono essere conservati in una forma che consenta l'individuazione dell'interessato per il tempo necessario agli scopi per cui sono stati raccolti, 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 (Art. 5 GDPR)

Si deve evitare di trattare i dati personali in presenza di terzi che possano così venire a conoscenza, anche occasionalmente, dei dati.
Si devono 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. Occorre informare tempestivamente e, in ogni caso senza ingiustificato ritardo, il proprio responsabile di ogni violazione di dati personali .di cui si viene a conoscenza (es. accessi non autorizzati al proprio PC o a banche dati, smarrimento di dati, cancellazione o modifica non autorizzata di dati..), utilizzando lo schema (**Allegato 6**).

In caso di assenza anche temporanea dall'ufficio, in particolare durante gli orari di accesso agli uffici da parte del pubblico esterno, il PC non deve essere lasciato incustodito e accessibile, ma deve essere spento o disconnesso o, in alternativa, oscurato con modalità salvaschermo (cd. screen-saver) dotato 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.
Il Dirigente di Settore/ Responsabile delegato può impartire ulteriori istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro.
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 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.
La violazione degli obblighi sopra considerati può comportare l'applicazione di sanzioni di natura disciplinare oltre ad eventuali responsabilità sotto il profilo amministrativo, civile e penale.

10. CONTRATTI / CONVENZIONI CON SOGGETTI ESTERNI (DITTE, COOPERATIVE, PROFESSIONISTI, SOGGETTI PUBBLICI, GESTORI DI PUBBLICI SERVIZI....)

- **NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI**

Il Comune rimane il Titolare del trattamento dei dati, pertanto, il Dirigente di settore titolare della banca dati, congiuntamente al Dirigente del settore/ servizio contraente, nomina il soggetto esterno in qualità di Responsabile esterno del trattamento, utilizzando l'apposito modello **(Allegato 4)**

- **NOMINA DELL' AMMINISTRATORE DI SISTEMA ESTERNO**

Il Responsabile esterno 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.

- **ACCESSO AD APPLICAZIONI E BANCHE DATI DEL SETTORE CONTRAENTE**

Il Responsabile esterno del trattamento fornisce al dirigente del settore che ha stipulato il contratto/convenzione l'elenco degli incaricati al trattamento dei dati per i quali richiede l'accesso. Il Dirigente del settore contraente/ Responsabile delegato attraverso l'apposita procedura informatica , accedendo da Profilo utente - Abilitazioni , comunica al preposto alla gestione delle credenziali, in particolare:

a) a quali applicazioni e banche dati ogni incaricato deve esser abilitato richiedendo altresì, se necessario, l'accesso ad Internet e l'utilizzo della posta elettronica;
b) la data di scadenza del contratto/ convenzione, se in suo possesso.

Il preposto alla gestione fornisce ad ogni incaricato le credenziali di autenticazione ed abilita all'accesso alle banche dati ed alle applicazioni richieste.

- **ACCESSO AD APPLICAZIONI E BANCHE DATI DI ALTRI SETTORI**

Qualora l'oggetto del contratto / convenzione comporti l'utilizzazione di banche dati di competenza di più settori, la designazione del responsabile dovrà essere sottoscritta congiuntamente dal dirigente del settore contraente e dai dirigenti delle banche dati interessate.
In questo caso, nella richiesta di abilitazione degli incaricati da inviare al preposto alla gestione

con le medesime modalità indicate al punto precedente, il dirigente del settore contraente dovrà dare atto che i dirigenti dei settori interessati sono stati informati.

- **SCADENZA CREDENZIALI**

Le credenziali hanno un periodo massimo di validità pari alla durata del contratto/ convenzione e comunque non superiore a ventiquattro mesi, 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 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.

- **ULTERIORI ADEMPIMENTI**

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 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 e Sistemi, 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.

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.

ALLEGATO 1

NOMINA RESPONSABILE INTERNO

Dott.

Ufficio / Servizio

Oggetto: Designazione responsabile interno 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 sulla sicurezza dei dati personali, approvato con 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;

- Il Manuale per la gestione di una violazione di dati personali (data breach) approvato con deliberazione della Giunta Comunale n.....del.....;
- 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:
- procede, d'intesa con il Titolare, se richiesto, 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.
- riferisce tempestivamente al Titolare fatti e condizioni che possono incidere sul legittimo e regolare svolgimento delle attività di trattamento e, 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;

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

- riferisce tempestivamente al Titolare eventuali violazioni delle disposizioni legislative in materia e ad osservare scrupolosamente le prescrizioni contenute nel Manuale per la gestione di una violazione di dati personali (data breach) provvedendo a segnalare tempestivamente e, in ogni caso, senza ingiustificato ritardo, a responsabileprotezionedati@comune.modena.it ogni evento anomalo che possa determinare la violazione di dati personali di cui sia venuto a conoscenza. Per la segnalazione dovrà essere utilizzato il modello allegato A al Manuale per la gestione di una violazione di dati personali (data breach).

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;

-ad 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 2

NOMINA INCARICATO AL TRATTAMENTO

(per accedere a dati e applicazioni del proprio settore)

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 sulla sicurezza dei dati personali approvato con la deliberazione della Giunta Comunale n..... del …..;
- il Manuale per la gestione di una violazione di dati personali (data breach) approvato con la deliberazione della Giunta Comunale n. 245 del 29/5/2020;

- la determinazione del dirigente del Settore ….....n..... avente per oggetto: *"Applicazione delle disposizioni in materia di protezione dei dati personali per il Settore .....Aggiornamento del Registro dei trattamenti";*
- 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.
- Devono essere osservate scrupolosamente le prescrizioni contenute nel Manuale per la gestione di una violazione di dati personali (data breach) provvedendo a segnalare tempestivamente e, in ogni caso , senza ingiustificato ritardo , a responsabileprotezionedati@comune.modena.it ogni evento anomalo che possa determinare la violazione di dati personali. Per la segnalazione dovrà essere utilizzato il modello allegato A al Manuale per la gestione di una violazione di dati personali (

data breach) pubblicato nella sezione Privacy di intranet

Il Dirigente

del Settore ….....

Dott.....

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

Dott. ….....

ALLEGATO 3

NOMINA INCARICATO AL TRATTAMENTO

(per accedere a dati e applicazioni di un settore diverso da quello di appartenenza)

Sig.....

Settore .....

Oggetto: Autorizzazione al trattamento di dati personali

Il sottoscritto, 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;
- il 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, e successive modifiche ed integrazioni;
- 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 sulla sicurezza dei dati personali approvato con deliberazione della Giunta Comunale n.748 del 18/12/2018 e successive modifiche ed integrazioni ;
- il Manuale per la gestione di una violazione di dati personali (data breach) approvato con la deliberazione della Giunta Comunale n. 245 del 29/5/2020;
- la propria determinazione n..... avente per oggetto: .....

di concerto con il dirigente del Settore .....

autorizza

il dipendente in indirizzo alle seguenti operazioni di trattamento:

.....

A tal fine impartisce 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.
- Devono essere osservate scrupolosamente le prescrizioni contenute nel Manuale per

la gestione di una violazione di dati personali (data breach) provvedendo a segnalare tempestivamente e, in ogni caso , senza ingiustificato ritardo , a responsabileprotezionedati@comune.modena.it ogni evento anomalo che possa determinare la violazione di dati personali. Per la segnalazione dovrà essere utilizzato il modello allegato A al Manuale per la gestione di una violazione di dati personali (data breach) pubblicato nella sezione Privacy di intranet

Il Dirigente del Settore .....
Dott. .....

Il Dirigente del Settore .....
Dott. .....

Per Ricevuta

Modena ….....

ALLEGATO 4
NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO

Spett.le

OGGETTO: NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI CONTRATTO ----------

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 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)]/

b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679

c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

d) Gli allegati da I a IV costituiscono parte integrante delle clausole.

e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725.

f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679

Clausola 2

Invariabilità delle clausole

a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le

presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3

Interpretazione

a) Quando le presenti clausole utilizzano i termini definiti, nel regolamento (UE) 2016/679 tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 / o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4

Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

SEZIONE II

OBBLIGHI DELLE PARTI

Clausola 6

Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7

Obblighi delle parti

7.1.Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento

(UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2.Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3.Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679 . Su

richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

a) OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA: Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno [SPECIFICARE IL PERIODO] prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato.

OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE: Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [SPECIFICARE IL PERIODO], dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui

il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679

c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679 .

b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capoV del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8

Assistenza al titolare del trattamento

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a

meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

   1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

   2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

   3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

   4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679/

d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 e delle disposizioni di cui al Manuale per la gestione di una violazione di dati personali del Comune di Modena , tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1.Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il

responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679/devono essere indicate nella notifica del titolare del trattamento e includere almeno:

   1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

   2) le probabili conseguenze della violazione dei dati personali;

   3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

A tal fine, il Responsabile del trattamento, nel rispetto delle prescrizioni contenute nel Manuale per la gestione di una violazione dei dati personali del Comune di Modena, consultabile al link: https://www.comune.modena.it/amministrazione-trasparente/disposizioni-generali/atti-generali-1/gestione-violazione-di-dati-personali-data-breach
che si impegna a rispettare, informa il Titolare tempestivamente, senza ingiustificato ritardo, e comunque entro 24 ore dal momento in cui ne ha conoscenza, di ogni violazione di dati personali (cd. Data breach) compilando la scheda "Segnalazione allegato A" del suddetto Manuale e inviandola, se possibile via Pec, al Titolare e all'indirizzo responsabileprotezionedati@comune.modena.it *;* tale comunicazione 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. Il Responsabile è tenuto a fornire al Titolare tutta la collaborazione necessaria per consentirgli di adempiere agli obblighi previsti dalla normativa in materia di data breach .

c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679

SEZIONE III

DISPOSIZIONI FINALI

Clausola 10

Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del regolamento (UE) 2016/679 , qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

    1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

    2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento

(UE) 2016/679 ;

3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679 .

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole

e) 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

ALLEGATO I

Elenco delle parti

Titolare/i del trattamento: [Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. Nome: …

   Indirizzo: …

   Nome, qualifica e dati di contatto del referente: …

   Firma e data di adesione: …

Responsabile/i del trattamento [Identità e dati di contatto del/dei responsabili del trattamento

e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. Nome: …

   Indirizzo: …

   Nome, qualifica e dati di contatto del referente: …

   Firma e data di adesione: …

ALLEGATO II

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

…..... (es. utenti, dipendenti, cittadini ..)

Categorie di dati personali trattati

…..... (es. identificativi, anagrafici, fiscali, di salute, sensibili, gudiziari …)

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, (ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata, tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.)

…

Natura del trattamento

…

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

…

Durata del trattamento

…

…

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

---

ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati

NOTA ESPLICATIVA:

Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche. Esempi di possibili misure:

misure di pseudonimizzazione e cifratura dei dati personali

misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

misure di identificazione e autorizzazione dell'utente

misure di protezione dei dati durante la trasmissione

misure di protezione dei dati durante la conservazione

misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

misure per garantire la registrazione degli eventi

misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita

misure di informatica interna e di gestione e governance della sicurezza informatica

misure di certificazione/garanzia di processi e prodotti

misure per garantire la minimizzazione dei dati

misure per garantire la qualità dei dati

misure per garantire la conservazione limitata dei dati

misure per garantire la responsabilità

misure per consentire la portabilità dei dati e garantire la cancellazione]

Per i trasferimenti a (sub-)responsabili del trattamento, descrivere anche le misure tecniche e

organizzative specifiche che il (sub-)responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

ALLEGATO IV

Elenco dei sub-responsabili del trattamento

NOTA ESPLICATIVA:

Il presente allegato deve essere compilato in caso di autorizzazione specifica di sub-responsabili del trattamento [clausola 7.7, lettera a), opzione 1].

Il titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:

1. Nome: …

   Indirizzo: …

   Nome, qualifica e dati di contatto del referente: …

   Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento): …

2. …

ALLEGATO 5

INFORMATIVA

Comune di Modena

INFORMATIVA resa ai sensi degli articoli 13 e 14 del RGPD (Regolamento Generale Protezione Dati) 2016/679

La informiamo che :

a) Il titolare del trattamento è il Comune di Modena. Con provvedimento del Sindaco, il dott. ……... (sede ….. e.mail …..... , telefono …..) , è stato nominato titolare delle banche dati e del trattamento dei dati del settore ….. , in conformità ai principi dell'Ordinamento degli enti locali ed alle scelte fondamentali assunte dal Comune in materia organizzativa.

b) il Responsabile della protezione dei dati (RPD) potrà essere contattato all'indirizzo di posta elettronica responsabileprotezionedati@comune.modena.it o all'indirizzo pec casellaistituzionale042@cert.comune.modena.it

c) i dati personali che La riguardano, dei quali entriamo in possesso, sono trattati da questo Ente ai sensi di ……... *(va indicata la base giuridica del trattamento)* per le seguenti finalità istituzionali
…….....

d) il trattamento è improntato ai principi di correttezza, di liceità, di trasparenza e di tutela della Sua riservatezza e dei Suoi diritti

e) possono venire a conoscenza dei Suoi dati personali i dipendenti e i collaboratori, anche esterni, del titolare e i soggetti che forniscono servizi strumentali alle finalità di cui sopra (come, ad esempio, servizi tecnici). Tali soggetti agiscono in qualità di responsabili , autorizzati al trattamento e amministratori di sistema. . I dati personali potranno essere comunicati a ……..(*indicare i soggetti pubblici e/o privati o le categorie di destinatari)* . I Suoi dati non verranno diffusi *oppure* saranno diffusi mediante pubblicazione ……..

f) i Suoi dati verranno conservati per ……..... *(indicare il periodo di tempo) oppure* per il periodo necessario per la conclusione del procedimento, al termine del quale potranno essere conservati, con le modalità e nel rispetto delle disposioni 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,

g) Il conferimento dei dati personali è obbligatorio in quanto sussiste un obbligo legale/ contrattuale al riguardo *oppure* , in quanto, in mancanza di esso, non sarà possibile dare inizio al procedimento

h) Il trattamento dei Suoi dati personali avverrà con modalità informatiche e/o telematiche e/o cartacee , in modo da garantire la riservatezza e la sicurezza degli stessi. (*In caso di processo decisionale automatizzato – es profilazione -deve essere predisposta un'informativa specifica in cui vengono date informazioni sulla logica utilizzata e*

sull'importanza e le conseguenze previste per l'interessato)

i) il trattamento dei Suoi dati personali non verrà trasferito a un paese terzo o a un'organizzazione internazionale

Lei potrà in qualsiasi momento, esercitare i Suoi diritti:

- di accesso ai dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che La riguardano;
- di revocare il consenso, ove previsto; la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito prima della revoca;
- alla portabilità dei dati, ove previsto;
- di opporsi al trattamento;
- di proporre reclamo all'Autorità di controllo (Garante Privacy)

ALLEGATO 6

SEGNALAZIONE EVENTO ANOMALO

Al dirigente del Settore ….....

Al Responsabile per la protezione dei dati
responsabileprotezione dati@comune.modena.it

Oggetto: Segnalazione evento

1. Descrizione evento

….....
.....

2. Data evento

- il ….
- tra il … e il ….....
- in un tempo non ancora determinato
- dal …..... (ancora in corso)

3 . Luogo evento .....

4. Tipo di violazione

- Diffusione / accesso di dati non autorizzato o accidentale
- Modifica di dati non autorizzata o accidentale
- Impossibilità di accesso / perdita / distruzione non autorizzata o accidentale
– Altro: ….....

5. Causa della violazione

- Azione intenzionale interna
- Azione accidentale interna
- Azione intenzionale esterna
- Azione accidentale esterna
- Sconosciuta

- Altro ….....

6. Dispositivo oggetto della violazione

– Computer
– Dispositivo mobile
– Documento cartaceo
– File o parte di file
– Strumento di back up
– Rete
– Altro: ….....

7. Ubicazione del dispositivo

….....

7. Numero persone colpite dalla violazione dei dati personali

– Numero di interessati ….....
– Circa n..... interessati
– Numero non ancora definito di interessati

8. Categorie di interessati

– Dipendenti/ Consulenti
- Utenti / Contraenti
- Associati, soci, aderenti
- Soggetti che ricoprono cariche sociali
- Beneficiari / assistiti
- Minori
- Persone vulnerabili (vittime di violenza o abusi, rifugiati, richiedenti asilo)
- Categorie ancora non determinate
- Altro ….....

9. Volume dei dati personali oggetto della violazione

– Numero ….....

– Circa n.....
– Numero non ancora definito di dati

10. Categorie di dati coinvolti nella violazione

– Dati anagrafici (nome, cognome, data e luogo di nascita, codice fiscale, altro)
– Dati di contatto (numero di telefono, e.mail, indirizzo postale)
– Dati di accesso e di identificazione (username, password, altro ….)
- Dati riferiti alla fornitura di un servizio
- Dati di profilazione
– Dati di localizzazione
- Dati di pagamento (es. numero conto corrente, dettagli carta di credito)
- Dati riferiti a persone fisiche vulnerabili (es. minori)
– Dati sensibili (specificare ….)
– Dati giudiziari (specificare …..)
– Dati relativi alla salute e all'orientamento sessuale
– Altro: ----------
– Ancora sconosciute

11. Ulteriori soggetti coinvolti nel trattamento

Contitolare ---------- codice fiscale/ partita IVA ….....

Responsabile esterno …..... codice fiscale/ partita IVA ….....

Data ….....

IL SEGNALANTE

.....