COMUNE DI XXXXXXXXXXXXXXXXXXXXX

ORDINANZA DIRIGENZIALE N. XXXX/XXXX

**OGGETTO: INCARICO AL TRATTAMENTO DEI DATI DEL SERVIZIO XXXXXXXX – SIGNOR XXXXXXXXXX**

 **IL DIRIGENTE.**

PRESO ATTO che con decreto n. XXXX/XX il Dott. XXXXXXX è stato nominato Incaricato del trattamento dei dati relativi al servizio XXXXXX dell’Ente;

VISTA la Deliberazione di Giunta comunale n. xx/XXX, che apporto modifiche alla struttura organizzativa dell’Ente;

RITENUTO che occorre aggiornare la nomina del Dott. Xxxxx quale Incaricato del Trattamento dei dati, rendendola conforme alla nuova organizzazione dell’Ente;

CONSIDERATO che, a seguito di apposita attività conoscitiva e valutativa è risultato che il dott. XXXXXoffre garanzie sufficienti circa le proprie qualità professionali e personali, in particolare esperienza, capacità e affidabilità nella conoscenza della base normativa (Regolamento UE 2016/679) e delle prassi in materia di protezione dei dati personali, nonché della capacità di assolvere i compiti con scrupolosità e diligenza;

In qualità di Responsabile del Trattamento dei Dati dei servizi di XXXX del Comune di XXXXXX

**NOMINA**

**XXXXX codice fiscale XXXXXXX**, **Persona Autorizzata** (art. 4 Regolamento UE 2016/679) ai trattamenti in allegato riportati secondo le istruzioni e i permessi accordati di seguito:

La Persona Autorizzata alla amministrazione di sistema degli strumenti elettronici si impegna a:

1. Garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli e a non divulgare, neanche dopo la cessazione dell’incarico, alcuna delle informazioni di cui è venuto a conoscenza nell’adempimento dei compiti assegnatigli (art. 28 par. 3 lettera b Regolamento UE 2016/679);
2. gestire il sistema informatico in osservanza dei principi generali del Regolamento UE 2016/679, attenendosi anche alle disposizioni generali del titolare (e di quelle specifiche del responsabile, qualora nominato) del trattamento in tema di sicurezza;
3. predisporre ed aggiornare un sistema di sicurezza informatico idoneo a rispettare principi e le prescrizioni normative specifiche, adeguandolo di volta in volta alle vigenti norme in materia di sicurezza;

Più specificatamente, la Persona Autorizzata all’amministrazione di sistema degli strumenti elettronici dovrà:

•attribuire a ciascuna persona autorizzata un codice identificativo personale per l’utilizzo degli elaboratori o del software di qualunque tipo o delle base dati. Il codice identificativo assegnato deve consentire l’accesso alle sole informazioni necessarie all’attività della persona autorizzata e deve poter essere autonomamente sostituita;

•attribuire alle persone autorizzate le parole chiavi relative al singolo sistema di elaborazione ovvero al singolo programma informatico per il trattamento dei dati effettuato con sistemi automatizzati;

•provvedere, su richiesta dei responsabili del personale, alla revoca o modifica dei codici identificativi;

•provvedere affinché gli elaboratori siano protetti dai rischi di intrusione ad opera di agenti di alterazione (o virus informatici) mediante idonei programmi informatici;

•procedere alla custodia dei supporti di memorizzazione e alla loro distruzione quando non utilizzati;

•provvedere alla corretta effettuazione delle operazioni di backup dei sistemi e delle banche dati e predisporne la relativa documentazione;

•comunicare alle persone autorizzate, e tenere aggiornate, le norme di comportamento per il corretto utilizzo dei sistemi automatizzati;

•controllare che soggetti non autorizzati non possano avere accesso agli archivi automatizzati;

•fornire alle persone autorizzate le istruzioni per la corretta selezione e l’utilizzo delle parole chiavi e vigilare sul corretto utilizzo delle stesse;

•cooperare nella predisposizione della documentazione in materia di protezione dei dati personali (es. registri dei trattamenti) per la parte concernente il sistema informatico ed il trattamento informatico dei dati;

•vigilare sugli interventi informatici diretti al sistema informatico del Comune e, se presente, sull’impianto di videosorveglianza effettuati da vari operatori esterni. In caso di anomalie sarà sua cura segnalarle tempestivamente al Titolare del Trattamento o al Responsabile del Trattamento o al Responsabile della Protezione dei Dati;

•predisporre ed implementare le eventuali ulteriori misure minime di sicurezza necessarie a garantire il rispetto delle norme per il trattamento informatico dei dati;

•comunicare prontamente al Titolare del Trattamento, o al Responsabile del Trattamento o al Responsabile della Protezione dei Dati, qualsiasi situazione di cui sia venuta a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali al fine di dare il via alla procedura di Data Breach;

•verificare il rispetto delle norme sulla tutela del diritto d’autore sui programmi e software installati nei dispositivi di qualsiasi tipo quali ad esempio PC, Tablet, smartphone;

•adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate come persone autorizzate alla amministrazione di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo “username” utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

L'Incaricato del Trattamento si impegna a:

• trattare i dati personali soltanto su istruzione documentata del Responsabile del Trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto l'Incaricato del trattamento, in questa circostanza l'Incaricato del Trattamento informa il Responsabile del Trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

• garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

• adottare tutte le misure richieste per la sicurezza del trattamento;

• assistere il Responsabile del trattamento con misure tecniche e organizzative adeguate, tenendo conto della natura del trattamento e nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Responsabile del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;

• assistere il Responsabile del trattamento nel garantire il rispetto degli obblighi relativi alla sicurezza dei dati personali e alla valutazione di impatto sulla protezione dei dati e consultazione preventiva;

• su scelta del Responsabile del trattamento, cancellare o restituire tutti i dati personali al termine della prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dei membri preveda la conservazione dei dati;

• mettere a disposizione del Responsabile del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi discendenti dalla normativa, consentire e contribuire all’attività di revisione, comprese le ispezioni, realizzati dal Responsabile del trattamento o da un altro soggetto da questi incaricato.

**Istruzioni ricevute dal Responsabile:**

Nello svolgimento del trattamento devono essere osservate le norme di legge e di regolamento in materia di tutela della riservatezza dei dati personali e devono essere applicate tutte le misure di sicurezza previste dalla legge e le relative istruzioni dell’Amministratore del Sistema, nonché del Responsabile del trattamento devono essere scrupolosamente osservate.

Il trattamento dei dati deve rispettare il principio di pertinenza e non eccedenza rispetto alle finalità del medesimo: è consentito l’accesso ai soli dati personali la cui conoscenza sia strettamente indispensabile per adempiere i compiti affidati.

I dati devono essere trattati in modo lecito e secondo correttezza ed essere esatti ed aggiornati. L'Incaricato, in particolare, nello svolgimento del trattamento, è tenuto ad applicare le seguenti istruzioni:

• accertare che l’informativa sul trattamento dei dati personali, completa in tutte le sue parti, venga comunicata agli interessati e verificare che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni;

• consentire l’esercizio dei diritti e delle facoltà previste [dall’art. 7 del D.lgs. n. 196/2003](http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto:2003-06-30;196~art7!vig=) (e cioè fornire conferma, all’interessato, dell’esistenza o meno dei dati che lo riguardano; indicare le finalità e modalità del trattamento ed ogni altra attività connessa allo stesso; provvedere, previa espressa richiesta informale e scritta dell’interessato, all’aggiornamento dei dati nonché alla loro rettificazione, integrazione, cancellazione, trasformazione in forma anonima o al blocco qualora trattati in violazione della legge);

• collaborare, con gli altri incaricati del medesimo trattamento, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite;

• non trasmettere, a soggetti terzi, informazioni circa dati personali trattati. La comunicazione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Responsabile del Trattamento;

• accertarsi dell’identità del diretto interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato;

• riporre in archivio, al termine del periodo di trattamento, i supporti o i documenti, ancorché non definitivi, contenenti i dati personali;

• conservare i dati trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati;

• crittografare i dati con particolare requisiti di riservatezza;

• non creare per quanto possibile utenze anonime e nel caso siano esistenti creare e gestire un registro che assicuri l’imputabilità di chi ne fa uso;

• impostare le password con la complessità e la robustezza necessarie (per le utenze di dominio almeno 8 caratteri, password aging, password history). Nel caso di presenza di ospiti o personale di servizio sarà necessario:

• fare attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;

• evitare di allontanarsi dalla scrivania in presenza di ospiti o riporre i documenti e attivare il salvaschermo del PC con richiesta di immissione della password;

• non rivelare o far digitare la password al personale di assistenza tecnica;

• non rivelare le password, nessuno è autorizzato a chiederle;

• segnalare qualsiasi anomalia e stranezza al Responsabile del Trattamento.

**Trattamenti concernenti dati sensibili e giudiziari**

L'Incaricato è autorizzato al trattamento dei dati sensibili e giudiziari necessari al compito svolto. Ferma l’applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Responsabile del trattamento, si riportano alcune specifiche misure:

• non fornire dati o informazioni di carattere sensibile per telefono, qualora non si abbia certezza assoluta sull’identità del destinatario;

• evitare di inviare documenti in chiaro contenenti dati sensibili: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all’interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);

• i documenti, ancorché non definitivi, ed i supporti recanti dati sensibili o giudiziari, devono essere conservati, anche in corso di trattamento, in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza dell’Incaricato;

• i supporti ed i documenti, recanti dati relativi alla salute e alla vita sessuale, devono essere conservati nei predetti contenitori muniti di serratura, separatamente da ogni altro documento;

• per la redazione, la pubblicazione, la comunicazione ed il rilascio degli atti recanti dati idonei a rivelare lo stato di salute, devono essere osservate tutte le norme di legge e di regolamento.

Per quanto riguarda, in particolare, le elaborazioni e le altre fasi dei trattamenti effettuate attraverso strumenti informatici, ciascun Incaricato disporrà di una parola chiave per l’accesso ai dati e di un codice identificativo personale. Gli Incaricati avranno cura di:

• non condividere il proprio codice identificativo personale con altri utenti, salvo i casi espressamente previsti;

• non cedere a terzi la propria parola chiave di autenticazione;

• non accedere a servizi non consentiti;

• non caricare ed eseguire software di rete o di comunicazione, senza previa verifica dello stesso da parte del proprio Referente informatico, che opera in stretto rapporto con il Servizio CED;

• non tentare di acquisire i privilegi di Amministratore di sistema;

• verificare l’assenza di virus nei supporti utilizzati;

• non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete;

• memorizzare i dati di interesse lavorativo sui server di condivisione, ove disponibili; in caso contrario, effettuare il backup periodico per i trattamenti non gestiti dall’Ufficio CED;

• procedere alla cancellazione dei supporti magnetici od ottici contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;

• attenersi alle istruzioni specificate attraverso circolari dell’ufficio privacy.

IL DIRIGENTE

**Banche dati**

La visione dei dati, contenuti nelle banche dati, esclude comunque qualsiasi forma di comunicazione, diffusione e trattamento degli stessi che non sia strettamente funzionale all’espletamento dei compiti d’istituto e che non si svolga nei limiti stabiliti da leggi e regolamenti.

**Trattamenti senza strumenti elettronici**

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati devono essere conservati per la durata del trattamento e successivamente riposti in archivi ad accesso controllato, secondo quanto sarà indicato di volta in volta, al fine di escludere l’accesso, agli stessi, da parte di persone non incaricate al trattamento. Nel caso di trattamento di dati sensibili o di dati giudiziari, gli atti e i documenti, contenenti i dati affidati agli Incaricati del trattamento, devono essere conservati in contenitori muniti di serratura, al fine di escludere l’acquisizione, degli stessi, da parte di persone non incaricate del trattamento. Qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi “distruggi documenti”; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili. Gli Incaricati sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto. Analogamente, per quanto riguarda i flussi di documenti cartacei all'interno degli uffici comunali, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse). Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell’ipotesi di cessazione del rapporto di lavoro, l'Incaricato perde i privilegi di accesso ai dati personali attribuiti all’ufficio di provenienza; la nomina si intenderà revocata con la cancellazione dell’Incaricato dall’elenco informatizzato dei trattamenti.

Il presente atto diventa esecutivo dalla notifica all’interessato.