Città Metropolitana di Messina

Il Segretario Generale

Prot. n. 1730/SG

Messina, 14/12/2018

Ai Responsabili dei Servizi

e p.c. Al Sindaco Metropolitano

Al Commissario Straordinario

L O R O S E D I

OGGETTO: Istruzioni operative per gli incaricati del trattamento in materia di applicazione del GDPR (Regolamento UE 679/16).

Si comunica che nella seduta della Conferenza dei Dirigenti allargata, tenutasi in data 13 dicembre 2018, sono state condivise le istruzioni operative da impartire agli incaricati del trattamento in materia di applicazione del GDPR (Regolamento UE 679/16) che si allegano alla presente.

Si invitano, pertanto, tutte le Posizioni Organizzative a darne massima diffusione nell'ambito dei Servizi di appartenenza provvedendo al contempo ad avviare tavoli informativi e formativi sull'argomento.

Degli incontri che i Responsabili dei Servizi avranno cura di coordinare dovrà essere garantita informazione alla sottoscritta, ai Dirigenti, al DPO e al Responsabile della transizione alla modalità operativa digitale, individuato con decreto sindacale n. 7 del 11/01/2018,.

Distinti saluti

F.to IL SEGRETARIO GENERALE
avv. Maria Angela Caponetti

(Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 D.L. 39/1993)

Città Metropolitana di Messina

(ai sensi della L.R. n. 15 del 4 agosto 2015)

Disposizioni organizzative per gli incaricati del trattamento in materia di applicazione del GDPR (Regolamento UE 679/16): istruzioni operative

Premessa

Il presente documento contiene le istruzioni operative per gli incaricati del trattamento dei dati personali della Città Metropolitana di Messina, conformemente al Regolamento (Ue) 2016/679 (GDPR), alla normativa nazionale in vigore, e per quanto attiene all'uso degli strumenti informatici, al "Regolamento per l'utilizzo dei servizi e delle attrezzature informatiche" già adottato dall'Ente con la deliberazione del Commissario Straordinario con i poteri del Consiglio Metropolitano n.16 del 22 maggio 2018. I dipendenti, i collaboratori, gli amministratori e in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relative ai dati devono ispirarsi a principi generali di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'Ente diverso da finalità strettamente istituzionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Ente.

1. Definizioni

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un dato come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. Adempimenti

Ciascun incaricato del trattamento deve:

- Rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- Rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- Utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e a utilizzare gli strumenti aziendali;
- Rispettare le misure di sicurezza idonee adottate dall'Ente, atte a salvaguardare la riservatezza e l'integrità dei dati;
- Segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- Accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- In caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- Mantenere riservate le proprie credenziali di autenticazione;
- Svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- Rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- Informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- Raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- Eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. Modalità di svolgimento delle operazioni

Le principali operazioni degli incaricati del trattamento sono:

- Identificazione dell'interessato:
  al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, e procedere correttamente alla raccolta e alla registrazione delle informazioni;
- Verifica del controllo dell'esattezza del dato e della corretta digitazione:
  al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e

all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:
  I locali, ove sono custoditi i dati personali (e in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. In caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, occorre adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'Ente. Laddove si esegue il trattamento di dati personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei e i supporti rimovibili contenenti tali dati. Al termine dell'orario lavorativo, ove la dinamica delle attività e il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali.
- Rilevazione presenze:
  ogni incaricato è tenuto a utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

4. Istruzioni per l'uso degli strumenti informatici

I dispositivi di memorizzazione del proprio PC e le unità di rete devono contenere informazioni strettamente professionali e non possono essere utilizzati per scopi diversi (immagini, video e documenti personali).
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

a) Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (personal computer, periferiche, lettori di smart card, ecc.). E' necessario adottare le misure di sicurezza per la tutela della riservatezza, onde evitare l'accesso ai dati da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione da parte dell'amministratore di sistema, mediante la raccolta e l'analisi di dati aggregati e anonimi. Nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, lo stesso amministratore di sistema procederà alla verifica delle registrazioni delle sessioni di lavoro per relazionare al Dirigente di competenza le condotte indebite, ovvero, su richiesta, comunicare all'autorità giudiziaria le informazioni senza alcuna ulteriore informativa all'interessato.
Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

- Al termine delle ore di servizio, il PC venga spento, a meno che non stia svolgendo elaborazioni automatiche particolari (procedure batch). In tal caso gli uffici devono essere tassativamente chiusi a chiave;
- Qualora l'incaricato si assenti anche momentaneamente dalla propria postazione, dovrà accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile ad altre persone. Pertanto provvederà a chiudere la sessione di lavoro sul PC con la funzione di logout, oppure, in alternativa, dovrà attivare un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
- Relativamente all'utilizzo dello screen-saver, questo non deve mai essere disattivato; il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC ovvero deve essere messo in funzione manualmente ogni volta che si lasci il PC incustodito e acceso;
- Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le stesse regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- Il PC portatile non deve essere mai lasciato incustodito;
- Per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno;

- In caso di furto è necessario avvertire tempestivamente il responsabile dei Servizi Informatici, onde prevenire possibili intrusioni nel sistema dell'Ente;
- Eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) e una parola chiave (password). L'adozione della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

- Tutela l'utilizzatore e in generale l'Azienda da accessi illeciti, atti di vandalismo, violazioni e danneggiamenti del patrimonio informativo;
- Tutela l'incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome utiiizzando le sue user id e password, cosicchè solo lui possa svolgere determinate azioni;
- Serve a gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere la password in base ai seguenti criteri:

- Deve essere lunga almeno otto caratteri;
- Non deve fare riferimento a informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro familiari;
- Deve contenere una combinazione di numeri, segni speciali, lettere, maiuscole e minuscole;
- Non deve essere uguali alle precedenti.

Per la corretta gestione della password inoltre è necessario:

- Modificarla almeno ogni 3 mesi;
- Sostituire al primo utilizzo ogni password provvisoria;
- Conservarla in luogo sicuro;
- Non rivelarla o condividerla con i colleghi di lavoro, familiari e amici, e soprattutto tramite il telefono;
- Non utilizzare la funzione, prevista da alcuni software, che consente di salvarla automaticamente per i successivi utilizzi della stessa applicazione.

c) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, può essere eseguiti solamente dalle persone dei Servizi Informatici su mandato del suo Responsabile o del Responsabile del trattamento. Pertanto gli utenti dei PC sono tenuti a rispettare i seguenti divieti:

- Non utilizzare sul PC dispositivi personali, o comunque non di proprietà dell'Ente;
- Non installare sistemi per connessione esterne (modem, wifi) poichè tali connessioni potrebbero aggirare i sistemi preposti alla sicurezza della rete aziendale, aumentando sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi non licenziati, e in generale tutti i software non autorizzati dai Servizi Informatici;
- Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

d) Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità istituzionali dell'Ente e in stretta connessione con l'effettiva attività e mansioni del dipendente che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza dell'azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- Quando si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione senza nemmeno aprire il contenuto;
- Non utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la mail debba essere utilizzata per la trasmissione di dati particolari (dati sensibili), si raccomanda di prestare attenzione affinché l'indirizzo del destinatario sia stato correttamente digitato, l'oggetto

del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile e nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

e) Gestione del salvataggio dei dati

Per i dati e i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, i Servizi Informatici eseguono salvataggi periodici affinché si possano ripristinare in toto oppure selettivamente eventuali file distrutti per guasti hardware oppure per cancellazioni involontarie.

f) Trasferimento dei dati

Il trasferimento di file contenenti dati personali, dati particolari (dati sensibili) o giudiziari su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (dati sensibili) o giudiziari devono essere crittografati.

g) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al sistema informatico causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Ente è installato un software antivirus aziendale che si aggiorna automaticamente. Questo non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso in cui il programma antivirus installato sul proprio PC riscontri la presenza di un virus, ovvero se ne sospetti la presenza, anche se non rilevata dal programma, è necessario darne immediatamente segnalazione al responsabile dei Servizi Informatici.
Si raccomanda di non scaricare, né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

Per quanto non espressamente specificato, si rimanda al "Regolamento per l'utilizzo dei servizi e delle attrezzature informatiche" adottato dall'Ente.

5. Istruzioni per l'uso degli strumenti "non elettronici"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (dati sensibili) o giudiziari che si ritiene debbano essere eliminati, devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), o l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (dati sensibili) o giudiziari, il rispetto di queste norme è obbligatorio.

a) Distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzano strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti dati personali richiede la presenza di misure di sicurezza con le quali l'incaricato possa interagire e una serie di accorgimenti direttamente gestibili dall'incaricato stesso. In particolare, si richiede:

- L'uso tassativo di armadi e cassetti dotati di serratura adeguata;
- L'utilizzo, ove si richieda la distruzione di documenti contenenti dati particolari (dati sensibili) o giudi-

ziari, di un trita-documenti.

c) Prescrizioni per gli incaricati

L'incaricato deve attenersi alle seguenti prescrizioni:

- In nessun caso è concesso l'accesso a documentazione contenente dati personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- La documentazione contenente dati personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- L'accesso ai supporti deve essere limitato al tempo necessario a svolgere i trattamenti previsti;
- I supporti devono essere archiviati in ambienti ad accesso controllato;
- I documenti contenenti dati personali non devono essere lasciati incustoditi in ambienti non controllati (ad es. a seguito della stampa dei documenti su stampante di rete);
- Il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro;
- Cassetti e armadi contenenti documentazione riservata devono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- L'accesso fuori orario lavorativo a documenti contenenti dati particolari (dati sensibili) o giudiziari può avvenire da parte di personale incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- La distruzione di documenti contenenti dati personali deve essere operata, ove possibile, direttamente dal personale incaricato;
- Ove non siano disponibili strumenti per la distruzione dei documenti (trita-documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale incaricato che avvia al macero la documentazione è tenuto a confezionarla in modo che il pacco risulti anonimo e solido;
- Quando gli atti e i documenti contenenti dati personali, dati particolari (dati sensibili) o giudiziari sono affidati agli incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti debbono essere controllati e custoditi dagli incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e quindi restituiti al termine delle operazioni affidate;
- L'accesso agli archivi contenenti dati particolari (dati sensibili) o giudiziari deve essere controllato. Se gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
- E' severamente vietato utilizzare documenti contenenti dati personali, dati particolari (dati sensibili) o giudiziari come carta da riciclo o da appunti.

6. Addetti alla manutenzione

I preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento, nonché gli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici, sono tenuti a:

- Effettuare operazioni di manutenzione e supporto per la verifica del corretto funzionamento (monitoraggio e diagnostica) dei flussi dei dati;
- Gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
- Gestire i profili di autorizzazione degli incaricati al trattamento dei dati su specifiche impartite dai responsabili di funzione e su indicazione dell'Amministratore di sistema;
- L'Amministratore di sistema provvederà alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei Responsabili ovvero della Direzione del Personale;
- Custodire la documentazione cartacea prodotta nello svolgimento dei propri compiti istituzionali;

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico. A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal Titolare, secondo le seguenti istruzioni operative:

- Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stam-

panti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare file già esistenti ma creare file di prova.

- Nel caso si renda strettamente necessario accedere a file contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
- Nell'effettuazione di operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, questi dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
- E' obbligatorio adottare le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
- E' necessario informare al più presto il Titolare o il Responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
- Proteggere con password tutti i dati contenuti nei database.

Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

- In presenza dell'incaricato, far digitare la password all'incaricato stesso, evitando di venirne a conoscenza;
- In assenza dell'incaricato, rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario, il quale provvederà all'inserimento della password.
- Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'Amministratore di sistema o provvedere, con la sua collaborazione, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione del sistema informatico

L'Amministratore di sistema ha facoltà, in qualunque momento, di controllare e verificare l'operato degli addetti alla manutenzione;
Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
L'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di ID e password;
E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dall'Ente, se non previa espressa comunicazione scritta;
Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali, deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni in materia di misure minime di sicurezza

7. Osservanza delle disposizioni in materia di protezione di dati personali

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

8. Inosservanza delle disposizioni e dei Regolamenti dell'Ente

Il mancato rispetto o la violazione delle regole contenute nelle presenti disposizioni organizzative comportano l'avvio di provvedimenti disciplinari e delle eventuali azioni civili e penali consentite.

9. Aggiornamento e revisione

Le disposizioni qui contenute sono soggette a revisione in caso di modifiche normative o ulteriori integrazioni organizzative.