CITTÀ DI LAMEZIA TERME
(provincia di Catanzaro)

LINEE GUIDA E MODELLI DI DESIGNAZIONE DI INCARICATI AUTORIZZATI AL TRATTAMENTO E AMMINISTRATORI DI SISTEMA

Titolare Trattamento: Comune di Lamezia Terme

Approvato con delibera di Giunta Comunale n. 191 del 09/06/2023

INTRODUZIONE

Passaggio fondamentale per l'attuazione del Regolamento Generale sulla Protezione dei Dati (GDPR), Regolamento (UE) 2016/679 è la nomina e la designazione delle figure che ruotano intorno al Titolare del Trattamento dei dati personali.

Il presente documento raccoglie i risultati di tale attività di revisione, proponendo i seguenti modelli di nomina e designazione:

- Modello di designazione delle persone autorizzate al trattamento (collaboratori interni);
- Modello di designazione delle persone autorizzate al trattamento (collaboratori esterni);
- Modello di designazione degli amministratori di sistema.

DEFINIZIONI E ACRONIMI

Definizioni

Termine	Descrizione
Dato personale	Ex art. 4, comma 1 del GDPR, "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 identificativo 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	Ex art. 4, comma 2 del GDPR: "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"
Titolare del trattamento	Ex art. 4, comma 7 del GDPR: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"
Responsabile del trattamento	Ex art. 4, comma 8 del GDPR: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento"
Accountability	Ex art. 5, paragrafo 2 del GDPR: "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)". Il paragrafo 1 dell'art. 5 del GDPR riguarda i principi fondamentali che devono essere accuratamente applicati ai trattamenti di dati personali

Tabella 1 - Definizioni

Acronimi

Termine	Descrizione
GDPR	General Data Protection Regulation
DT	Delegato del Titolare / Responsabile del Trattamento Interno
RPD / DPO	Responsabile della Protezione dei Dati Personali / Data Protection Officer
AdS	Amministratore di Sistema

DESCRIZIONE GENERALE DEI MODELLI

Nomina dei responsabili dei trattamenti esterni

Vi sono situazioni in cui il Titolare del Trattamento ha la necessità di esternalizzare alcune attività di trattamento dei dati personali, avvalendosi di opportuni soggetti esterni che dovranno operare per conto del Titolare del Trattamento.

Al caso precedentemente esposto deve essere applicato lo schema di responsabilità ex art. 28 del GDPR: il soggetto esterno entra sostanzialmente a far parte del "sistema privacy" del Titolare, operando sotto la sua autorità. Tale impostazione del rapporto legittima il terzo ad utilizzare, per la parte di competenza, i dati che rientrano nel dominio del Titolare, vincolandolo però a standard prestazionali e di comportamento ben definiti. Il responsabile esterno conserva una parziale autonomia riguardante la sola concreta disciplina del servizio ed alcune scelte tecnico-operative, ma non anche le principali decisioni sulle finalità e sulle modalità di utilizzazione dei dati che spettano esclusivamente al Titolare del trattamento; il Responsabile esterno risponderà dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli art. 1218 e 1223 del Codice Civile. Nello stesso tempo il Titolare gestirà – mediante la relazione contrattuale connessa all'incarico – i dati personali del soggetto responsabile del trattamento.

Il presupposto per l'affidamento di trattamenti a soggetti esterni, è che sia valutata nella fase istruttoria (mediante acquisizione di specifica documentazione) l'affidabilità del soggetto: in relazione all'esperienza, capacità, alle misure di sicurezza organizzative e tecnico-informatiche affinchè fornisca adeguate garanzie del pieno rispetto delle disposizioni contenute nel GDPR.

Elementi utili al fine di ottenere un'efficace valutazione, possono essere:

- con riferimento ai requisiti di **capacità morale e di affidabilità**, l'assenza di condanne rilevanti in materia, ad es., con riferimento:
  - ✓ ad uno o più dei reati precedentemente previsti dal D.lgs. 196/2003 (artt. 167 e ss.) o dall'art. 24 bis del D.lgs. 231/2001 in relazione agli apicali dell'ente o direttamente in capo all'ente (sanzioni amministrative dipendenti da reato);
  - ✓ alle sanzioni amministrative in capo al Titolare del trattamento precedentemente previste dal GDPR (art. 83);

- con riferimento ai requisiti di **capacità tecnica**:
  - ✓ il possesso di sistemi certificati di gestione della sicurezza delle informazioni (es., ISO 27001), di continuità operativa (es., ISO 22301) ovvero la dichiarata adesione a Linee guida o Codici di condotta specifici (es., ISO 17799, ISO/IEC 27032, Codici di condotta specifici), in attesa di analoghi strumenti definiti ai sensi degli artt. 40 e ss. del Regolamento UE 679/2016;
  - ✓ l'attestazione di adozione dei controlli di natura tecnologica, organizzativa e procedurale definiti dalla Circolare AgID n. 2 del 18 aprile 2017 ''Misure minime di sicurezza ICT per le pubbliche amministrazioni'' (G.U. – Serie Generale n. 103 del 5 maggio 2017), a partire dal livello minimo (per la generalità dei casi, mentre i livelli superiori – Standard ed Alto – potrebbero essere utilizzati nei casi di trattamenti maggiormente impattanti);
  - ✓ idonea e documentata attestazione e descrizione delle misure di accountability adottate ai sensi del GDPR (ad es., registro dei trattamenti, nomina RPD) e delle misure di sicurezza organizzative e tecniche implementate ai sensi degli artt. 24 e 32 del Regolamento UE.

Le caratteristiche per la valutazione del soggetto esterno sono definite – in funzione della "criticità" delle attività da affidare - dal RUP ed oggetto di valutazione da parte del RUP stesso in caso di affidamento diretto, dalla Commissione di aggiudicazione, nel caso in cui sia prevista, o ancora dal soggetto preposto all'interno dell'ente con un atto deliberativo che formalizza gli accordi con la figura terza.

Designazione delle persone autorizzate al trattamento

Il GDPR non prevede esplicitamente il ruolo di chi materialmente effettua le operazioni di trattamento, tuttavia non ne esclude la designazione, facendo rientrare questa figura tra le "persone autorizzate al trattamento" dei dati sotto l'autorità diretta del titolare o del responsabile al quale il titolare ha delegato alcune delle proprie funzioni (Art.4 GDPR).

La persona autorizzata è la persona fisica che **effettua materialmente le operazioni di trattamento sui dati personali sotto l'autorità diretta del Titolare del Trattamento o del suo delegato**. Tali individui devono essere opportunamente scelti e preparati al fine di operare in maniera lecita, corretta e trasparente sui dati degli utenti.

L'incarico viene affidato attraverso una specifica lettera di designazione che riporterà i trattamenti che la persona autorizzata potrà svolgere nell'ambito dell'espletamento dei compiti della propria attività lavorativa.

Il Titolare del trattamento, con il supporto della funzione DPO ha predisposto due diversi modelli di designazione:

- modello di designazione delle persone autorizzate al trattamento per collaboratori interni all'ente;
- modello di designazione delle persone autorizzate al trattamento per collaboratori esterni all'ente, ma che operano comunque sui trattamenti sotto l'autorità diretta del Titolare del Trattamento.

Designazione degli amministratori di sistema

L'Amministratore di sistema viene definito nel Provvedimento del Garante del 27 novembre 2008 come "*una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali*". È da ritenersi questa la definizione più autorevole, poiché mancano ulteriori indicazioni normative in tal senso.

Il Garante Privacy per mezzo di tale provvedimento ha voluto far emergere all'interno del sistema di gestione per la protezione dei dati personali proprio di ogni organizzazione, il ruolo dell'Amministratore di Sistema evidenziandone la rilevanza e disponendo che i Titolari mettano in atto misure di sicurezza tecniche e organizzative prevedendo la selezione dei candidati sulla base di comprovate capacità tecniche, la successiva assegnazione agli Amministratori di adeguati livelli di responsabilità e la definizione di procedure volte a garantire la costante supervisione sul loro operato.

Non intervenendo il GDPR in materia di Amministratori di Sistema possiamo attenerci a quelle che sono state le indicazioni del Garante riguardo questa figura:

- Il Titolare è tenuto a designare individualmente i singoli Amministratori di sistema, con un atto che ne elenca gli ambiti di operatività.

- I Titolari sono tenuti a riportare in un documento interno le informazioni per identificare gli individui con ruolo di Amministratori di sistema, e l'elenco delle funzioni ad essi attribuite. Questo documento dev'essere consultabile dal Garante qualora ne faccia richiesta.

- Qualora i servizi di amministrazione di sistema siano esternalizzati, il documento di cui sopra deve essere conservato dal Titolare o dal Responsabile esterno del trattamento.

- Il Titolare deve adottare misure che consentano la registrazione degli accessi logici da parte degli Amministratori ai sistemi e agli archivi elettronici. L'accesso di ogni Amministratore deve essere registrato e conservato per almeno 6 mesi, con caratteristiche di completezza, integrità ed inalterabilità e deve comprendere anche gli estremi temporali, la descrizione dell'evento e del sistema interessato. Questo requisito, per il Comune di Lamezia Terme viene coperto dal sistema di Log Management ADS fornito da terzi.

- Qualora gli Amministratori nell'espletamento delle proprie funzioni trattino dati personali dei lavoratori, questi ultimi in qualità di interessati hanno diritto di conoscerne l'identità. È compito del Titolare rendere noto ai lavoratori dipendenti detto loro diritto.

- Alla luce del principio di "accountability" del GDPR l'operato degli Amministratori di sistema deve poter essere oggetto di verifica, con cadenza almeno annuale, al fine di verificare che le attività svolte dall'Amministratore siano conformi alle mansioni a lui attribuite.

In tale scenario l'Amministratore di sistema è una figura essenziale chiamata a svolgere funzioni che implicano la concreta capacità di accedere ai dati che transitano sulle reti aziendali ed istituzionali e, sempre a lui viene affidato il compito di vigilare sul corretto utilizzo dei sistemi informatici. Dovendo essere personale tecnico qualificato non potrà essere un ruolo che coincide con altre figure di controllo quale l'RPD che svolge autonome attività di audit nell'ambito della sicurezza informatica.

Seguono i modelli/template.

Modello di designazione delle persone autorizzate al trattamento (collaboratori interni)

Lettera di designazione a "Persona autorizzata al trattamento dei dati personali"
ai sensi dell'art. 4, comma 10, e dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies, comma 2, del decreto legislativo 30 giugno 2003, n. 196

Oggetto: **Designazione a "Persona autorizzata al trattamento dei dati personali"**

Al Sig._____nato a_____il_____, matricola_____ qualifica_____in forza all'Ufficio / Settore denominato in macrostruttura _____

PREMESSO

- Che il Comune di Lamezia Terme, in qualità di Titolare del Trattamento, ha delegato i compiti e funzioni di cui all'art. 2, comma 2 del Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, a ciascun Responsabile di Settore o Ufficio di diretta collaborazione, quali "Responsabili del Trattamento" (di seguito anche "Delegati del Titolare"), ognuno per le attività di trattamento dei dati personali effettuate nell'ambito dell'articolazione amministrativa di cui sono responsabili;
- che, nell'ambito dello svolgimento delle Sue funzioni, Lei viene necessariamente a conoscenza di una parte, sia pur limitata, dei dati contenuti nelle banche dati e negli archivi cartacei presenti in questa Amministrazione ed ai quali il Settore di cui fa parte ha specifico accesso;

CON LA PRESENTE

la S.V. è designata "Persona autorizzata al trattamento dei dati personali" (di seguito "Persona autorizzata"), ai sensi dell'art. 2-quaterdecies, comma 2, del decreto legislativo 30 giugno 2003, n. 196, e degli artt. 4, comma 10, e 29 del Regolamento UE 2016/679. La formalizzazione di tale designazione è indispensabile per attribuire specifiche responsabilità, a tutela della legittimità delle operazioni di trattamento dei dati personali, nell'ambito delle competenze dell'articolazione amministrativa, ed evitare che siano comminate sanzioni civili, amministrative e penali (salvo il caso di dolo o colpa) nei confronti di personale non autorizzato.

Si precisa che:

- per "**dato personale**" si intende, ai sensi dell'art. 4, comma 1 del Regolamento UE 2016/679, "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 identificativo 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";
- per "**trattamento**" si intende, ai sensi dell'art. 4, comma 2 del Regolamento UE 2016/679, "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".

In particolare, l'ambito del trattamento a Lei consentito è quello di competenza (dell'Ufficio di assegnazione), nei limiti di quanto necessario allo svolgimento delle attività a Lei affidate e riportati, per quanto possibile, nella seguente tabella per l'adempimento dei compiti assegnati:

Banca dati /Archivio cartaceo	DP[1]	DG[2]	Trattamenti[3]	Compiti	Rif. Registro trattamenti

Il trattamento dei dati dovrà essere effettuato nel rispetto della normativa comunitaria e nazionale vigente in materia di protezione dei dati personali, delle direttive/circolari fornite dal Titolare del Trattamento e delle istruzioni riportate nella presente lettera di designazione e successivamente nel corso della prestazione lavorativa.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati personali trattati permangono anche a seguito di modifica delle mansioni della Persona autorizzata o di cessazione del rapporto di lavoro.

Per tutto quanto non chiaramente specificato nella presente lettera di designazione, si rimanda al rispetto di quanto prescritto dal Regolamento (UE) 2016/679 (GPDR) e dal decreto legislativo 30 giugno 2003, n.196 e s.m.i. (Codice Privacy).

Le istruzioni impartite costituiscono elementi di valutazione della condotta del personale e l'inosservanza delle stesse può comportare forme di responsabilità disciplinare oltre che responsabilità penale e civile nei casi previsti dalla normativa.

A tal fine, vengono fornite **informazioni ed istruzioni** alle quali attenersi per l'effettuazione dei trattamenti assegnati.

Relativamente agli **aspetti generali** delle attività di trattamento:

- trattare i dati personali, in base all'art. 5 del GPDR, in modo lecito, corretto e trasparente, assicurando che siano:
    - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità ("limitazione della finalità");
    - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati"); limitare attentamente i trattamenti alle sole necessità funzionali ai propri compiti da assolvere, rispettando le direttive del Delegato del Titolare;

1 Dati personali particolari.
2 Dati personali giudiziari.
3 Abbreviazioni utilizzabili per la descrizione dei trattamenti principali:

- CREAZIONE - crea ed organizza l'archivio, raccoglie, registra ed inserisce nuovi dati;
- MODIFICA - modifica, estrae, elabora e cancella i dati;
- LETTURA - seleziona, raffronta e consulta i dati;
- COMUNICAZIONE - diffonde e comunica l'informazione;
- ARCHIVIAZIONE - archivia i dati;
- ELABORAZIONE - elabora e conserva i dati in formato digitale;
- TUTTI - effettua tutti i trattamenti previsti dal Delegato del Titolare.

- esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
- conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");
- adeguatamente protetti da trattamenti non autorizzati o illeciti e da perdite, distruzioni o danni accidentali ("integrità e riservatezza");

- nell'ambito dello svolgimento delle Sue mansioni, qualora si verificasse l'esigenza di modificare trattamenti esistenti o introdurre nuovi trattamenti non compresi nel Suo profilo di autorizzazione, informare prontamente il Responsabile del Suo Ufficio; qualora ne ricorrano le condizioni, Le sarà rilasciata esplicita autorizzazione, da parte del Delegato del Titolare, per procedere con le modifiche dei trattamenti in corso e/o con l'avvio dei nuovi trattamenti;
- recepire le indicazioni sui trattamenti, da parte del Delegato del Titolare, anche partecipando a percorsi formativi, quando previsti;
- controllare e custodire con diligenza, durante lo svolgimento delle operazioni di trattamento, gli atti, i documenti e i supporti informatici di memorizzazione contenenti dati personali, per evitarne la visione dei dati, l'acquisizione e l'utilizzo non autorizzato da parte di terzi;
- non conservare/duplicare/comunicare i dati personali, di cui si è venuti a conoscenza durante le operazioni di trattamento, dopo la revoca esplicita dell'autorizzazione o dopo la cessazione del rapporto di lavoro;
- non comunicare/diffondere i dati personali all'esterno dell'Amministrazione senza preventiva autorizzazione del Delegato del Titolare; il divieto permane anche dopo la cessazione della presente autorizzazione e/o del rapporto di lavoro; la trasmissione di dati all'interno dell'Amministrazione è consentita solo per i compiti ed i fini stabiliti dal Delegato del Titolare e agendo sotto la sua diretta autorità;
- non fornire per telefono dati e informazioni relativi alla salute, qualora non si abbia certezza dell'identità del destinatario;
- rispettare ed applicare le norme di sicurezza per la protezione dei dati personali;
- segnalare, al Delegato del Titolare, eventuali circostanze che richiedano un necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- informare tempestivamente il Delegato del Titolare di ogni questione di rilievo, in relazione ai trattamenti effettuati e alle eventuali richieste pervenute dagli interessati;
- informare immediatamente il Delegato del Titolare nel caso in cui si constati o si sospetti un disguido o un incidente che abbia messo o possa mettere a repentaglio la sicurezza dei dati trattati;
- garantire agli interessati l'esercizio dei diritti sui propri dati secondo quanto previsto dal GDPR (diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, etc.);
- in caso di allontanamento dalla propria postazione di lavoro, adottare tutte le cautele necessarie atte ad evitare l'accesso, da parte di terzi non autorizzati, ai dati personali trattati sia in formato elettronico che cartaceo;
- senza previa autorizzazione del Responsabile del Suo Ufficio, non effettuare in alcun modo, di propria iniziativa, collegamenti di dispositivi mobili personali alla rete dati e/o ai PC dell'Ente;
- senza previa autorizzazione del Responsabile del Suo Ufficio, non trasferire in alcun modo, di propria iniziativa, materiale in formato elettronico o cartaceo, contenente dati personali ed afferenti l'attività lavorativa svolta, in luoghi esterni all'ufficio;
- nel caso di lavoro agile, seguire le raccomandazioni fornite dal Titolare relativamente alle Raccomandazioni di sicurezza nell'utilizzo di informazioni e strumenti tecnologici;
- fornire al Delegato del Titolare, a semplice richiesta o secondo le modalità indicate da questo, tutte le informazioni relative all'attività svolta, al fine di consentirgli un'adeguata azione di controllo;

Relativamente alle **misure di sicurezza** da adottare per ottemperare alle prescrizioni di cui al precedente paragrafo, fermo restando quanto previsto dal DISCIPLINARE SULL'USO DELLE RISORSE I.C.T. (information and communication technology) Approvato con D.G. 606 del 30/12/2009, si riportano di seguito alcuni aspetti di dettaglio**:**

- **Archiviazione dati**
  - non archiviare dati personali direttamente sul PC;
  - non utilizzare supporti e/o servizi online personali di memorizzazione non forniti dalla struttura preposte ai sistemi informativi;
  - non lasciare chiavette USB, Hard Disk esterni o altri supporti di memorizzazione a disposizione di estranei; riporre i supporti di memorizzazione in modo ordinato negli appositi contenitori e chiudere a chiave i classificatori e gli armadi dove sono custoditi;
  - nel caso di supporti di memorizzazione già utilizzati per il trattamento di dati relativi alla salute, procedere al loro riutilizzo solo se le informazioni precedentemente contenutevi non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti;
  - evitare di gestire le stesse informazioni su più archivi (ove non sia necessario) e, nel caso, curarne l'aggiornamento in modo organico;
  - conservare i dati relativi alla salute in armadi chiusi e ad accesso controllato o in file protetti da password;

- **Codici di accesso / Credenziali**
  - accedere al sistema per mezzo di credenziali di autenticazione; le credenziali di autenticazione più comuni consistono in un codice identificativo (user id o username) per l'identificazione della Persona autorizzata e una parola chiave (password) conosciuta solo dalla Persona autorizzata;
  - utilizzare password robuste con, qualora il sistema lo permetta, lunghezza minima di otto caratteri, lettere maiuscole, lettere minuscole, numeri e caratteri speciali (ad es., simboli di punteggiatura);
  - evitare di creare password con elementi o notizie facilmente riconducibili alla propria persona;
  - nel caso di password assegnata dall'Amministratore di Sistema, modificarla al primo utilizzo e ogni volta che viene richiesto dal sistema o nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza;
  - qualora il sistema non renda obbligatorio la modifica periodica della password, provvedere autonomamente a tale variazione sulla base delle indicazioni fornite dalla struttura preposta ai sistemi informativi;
  - adottare particolari cautele per assicurare la segretezza delle password, evitando ad esempio di essere osservati durante la digitazione e conservando i riferimenti in luoghi non accessibili a terzi;
  - per l'accesso alle banche dati telematiche, utilizzare sempre i propri codici di accesso personali, per consentire sempre la corretta individuazione dell'autore del trattamento, evitando di operare su terminali altrui e/o lasciare aperta la sessione di lavoro con i propri codici di accesso inseriti;

- **Gestione dei dispositivi (Personal Computer)**
  - bloccare la sessione del PC ogni volta che ci si allontana dalla postazione di lavoro, sia per un tempo breve sia per un tempo più lungo, dovuto, ad esempio, ad una riunione, alla pausa pranzo o ad una missione fuori dalla sede di lavoro;
  - spegnere il PC alla fine della giornata lavorativa; nel caso in cui fosse necessario mantenere acceso il PC, assicurarsi di aver bloccato la sessione del PC;

- non alterare in alcun modo la configurazione software del proprio PC, evitando in particolare di installare qualsiasi software non autorizzato dall'Amministrazione e di modificare/disattivare le impostazioni dell'antivirus;
- qualora si dovessero riscontrare malfunzionamenti tecnici o anomalie nell'utilizzo del PC, segnalare al più presto tali eventi alla struttura preposta ai sistemi informativi;

- **Rete dati e posta elettronica**
  - utilizzare la rete dati di Comune di Lamezia Terme solo per fini espressamente autorizzati;
  - tenere un comportamento corretto durante la navigazione in Internet, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete;
  - prestare la massima cura e attenzione nell'invio di informazioni attraverso i sistemi di comunicazione elettronica, controllando accuratamente l'indirizzo dei destinatari ed essendo consapevoli del rischio che possano essere rese disponibili al pubblico;
  - non trasmettere via "e-mail standard" dati particolari o dati relativi a condanne penali o reati; i dati particolari riguardano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici identificativi, la salute, la vita sessuale, l'orientamento sessuale); nel caso in cui per ragioni d'ufficio sia strettamente necessaria tale forma di trasmissione, occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche; in particolare, si raccomanda il ricorso all'uso di tecniche di cifratura dei messaggi (file protetti da password, etc.);
  - evitare di aprire o fare il download di documenti ricevuti di cui non sia certa la provenienza; nel dubbio consultare la struttura preposta ai sistemi informativi;

- **Trattamenti cartacei**
  - garantire sempre la corretta custodia dei documenti; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altre Persone autorizzate addette al medesimo trattamento; i documenti non possono essere riprodotti o fotocopiati, se non per esigenze connesse alle finalità del trattamento; i documenti non devono essere consultati da persone non autorizzate al trattamento;
  - conservare i documenti o gli atti, che contengono dati particolari e/o giudiziari, in archivi ad accesso controllato, come ad es. armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di personale preposto;
  - restituire tempestivamente la documentazione prelevata dagli archivi, al termine delle operazioni di trattamento;
  - in caso di utilizzo di stampanti, fotocopiatrici o fax, condivisi da vari utenti e collocati al di fuori dei locali ove è posta la propria postazione di lavoro, raccogliere e custodire immediatamente, con le modalità sopra descritte, tutte le stampe prodotte;
  - distruggere opportunamente le copie cartacee non più utili di documenti contenenti dati personali, evitando di gettarli via così come sono;
  - adottare misure che siano idonee a limitare la conoscenza dei dati particolari e/o giudiziari qualora essi siano presenti nei flussi documentali dell'Amministrazione, garantendo il rispetto della riservatezza dei dati degli interessati.

- **Rapporti di front-office:**
  - rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello (cd. Front-office) deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;

- identificazione dell'interessato: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere (si pensi a soggetti stranieri ovvero a dati identificativi che possono generare dubbi sulla correttezza della registrazione) ovvero con riferimento alla personalità della prestazione richiesta: può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;
- controllo dell'esattezza del dato: fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbe creare problemi nella gestione dell'anagrafica e nel proseguo del processo;
- obbligo di riservatezza e segretezza: l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal Codice Privacy;

Cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- controllo dell'identità del richiedente: nel caso di richieste di comunicazione di dati (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti a mezzo intervista guidata;
  In alcuni casi, i Delegati del Titolare potrebbero disporre di comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);
- verifica dell'esattezza dei dati comunicati: nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione all'esattezza del dato che viene comunicato, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor;

- **<u>Istruzioni per l'uso degli strumenti del trattamento - Telefono</u>**

Nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

- chiedere l'identità del chiamante e la motivazione della richiesta;
- richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
- verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante (ad esempio caserma dei carabinieri, servizi pubblici e di PS, …);
- procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;

- **<u>Istruzioni per l'uso degli strumenti del trattamento - FAX</u>**

Nell'utilizzare questo strumento occorre prestare attenzione a:

- digitare correttamente il numero di telefono, cui inviare la comunicazione;
- controllare l'esattezza del numero digitato prima di inviare il documento;
- verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli contemporaneamente;

- attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
- qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
- in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;

- **<u>Istruzioni per l'uso degli strumenti del trattamento – SCANNER</u>**

I soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;

Resta inteso che la presente designazione avrà la medesima durata del Suo rapporto con Comune di Lamezia Terme e che, successivamente alla cessazione di tale rapporto, Lei non sarà più autorizzato ad effettuare alcun tipo di trattamento sui dati.

Lamezia Terme, li _____

Il Responsabile del Trattamento delegato dal Titolare

Letto firmato e sottoscritto per presa visione
dalla persona autorizzata

NOTE PER LA COMPILAZIONE DELLA TABELLA DEI TRATTAMENTI AUTORIZZATI

- **DP** - Indicare con "X" se si prevede l'accesso a dati personali particolari (relativi all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza sindacale, ai dati genetici, ai dati biometrici identificativi, alla salute, alla vita sessuale, all'orientamento sessuale).
- **DG** - Indicare con "X" se si prevede l'accesso a dati personali giudiziari (relativi a condanne penali e reati).
- **Trattamenti** - Descrivere i trattamenti autorizzati. È possibile fare riferimento anche ai seguenti trattamenti predefiniti, riportandone il nome indicato in lettere maiuscole:

– *CREAZIONE* - crea ed organizza l'archivio, raccoglie, registra ed inserisce nuovi dati;
– *MODIFICA* - modifica, estrae, elabora e cancella i dati;
– *LETTURA* - seleziona, raffronta e consulta i dati;
– *COMUNICAZIONE* - diffonde e comunica l'informazione;
– *ARCHIVIAZIONE* - archivia i dati;
– *ELABORAZIONE* - elabora e conserva i dati in formato digitale;
– *TUTTI* - effettua tutti i trattamenti previsti dal Delegato del Titolare.

- **Compiti** - Compiti lavorativi che necessitano dei trattamenti indicati.
- **Revoca** - Eventuale data di revoca della designazione rispetto ai trattamenti indicati.

Modello di designazione delle persone autorizzate al trattamento (collaboratori esterni)

Lettera di designazione a "Persona autorizzata al trattamento dei dati personali"
ai sensi dell'art. 4, comma 10, e dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies, comma 2, del decreto legislativo 30 giugno 2003, n. 196

Oggetto: **Designazione a "Persona autorizzata al trattamento dei dati personali"**

Al Sig._____nato a_____il_____, matricola_____ qualifica_____in forza all'Ufficio / Settore denominato in macrostruttura _____

PREMESSO

- Che il Comune di Lamezia Terme, in qualità di Titolare del Trattamento, ha delegato i compiti e funzioni di cui all'art. 2, comma 2 del Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, a ciascun Responsabile di Settore o Ufficio di diretta collaborazione, quali "Responsabili del Trattamento" (di seguito anche "Delegati del Titolare"), ognuno per le attività di trattamento dei dati personali effettuate nell'ambito dell'articolazione amministrativa di cui sono responsabili;
    - che il Comune di Lamezia Terme si avvale della Società _____ per i servizi di_____;
    - che tali servizi sono forniti ai sensi del Contratto/Convenzione n._____sottoscritto in data ___ e con scadenza in data_____;
- che, nell'ambito dello svolgimento delle Sue funzioni, Lei viene necessariamente a conoscenza di una parte, sia pur limitata, dei dati contenuti nelle banche dati e negli archivi cartacei presenti in questa Amministrazione ed ai quali il Settore _____ha specifico accesso;

CON LA PRESENTE

la S.V. è designata "Persona autorizzata al trattamento dei dati personali" (di seguito "Persona autorizzata"), ai sensi dell'art. 2-quaterdecies, comma 2, del decreto legislativo 30 giugno 2003, n. 196, e degli artt. 4, comma 10, e 29 del Regolamento UE 2016/679. La formalizzazione di tale designazione è indispensabile per attribuire specifiche responsabilità, a tutela della legittimità delle operazioni di trattamento dei dati personali, nell'ambito delle competenze dell'articolazione amministrativa, ed evitare che siano comminate sanzioni civili, amministrative e penali (salvo il caso di dolo o colpa) nei confronti di personale non autorizzato.

Si precisa che:

- per "**dato personale**" si intende, ai sensi dell'art. 4, comma 1 del Regolamento UE 2016/679, "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 identificativo 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";
- per "**trattamento**" si intende, ai sensi dell'art. 4, comma 2 del Regolamento UE 2016/679, "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".

La S.V. è autorizzata ad effettuare i trattamenti di dati personali riportati nella seguente tabella, accedendo ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati:

Banca dati / Archivio cartaceo	DP[4]	DG[5]	Trattamenti[6]	Compiti	Rif. Registro

Il trattamento dei dati dovrà effettuarsi nel rispetto della normativa comunitaria e nazionale vigente in materia di protezione dei dati personali, delle direttive/circolari e delle istruzioni riportate nella presente lettera di designazione e successivamente nel corso della prestazione lavorativa.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati personali trattati permangono anche a seguito di modifica delle mansioni della Persona autorizzata o di cessazione del rapporto di lavoro.

Per tutto quanto non chiaramente specificato nella presente lettera di designazione, si rimanda al rispetto di quanto prescritto dal Regolamento (UE) 2016/679 (GPDR) e dal decreto legislativo 30 giugno 2003, n. 196 e s.m.i. (Codice Privacy).

Le istruzioni impartite costituiscono elementi di valutazione della condotta del personale e l'inosservanza delle stesse può comportare forme di responsabilità disciplinare oltre che responsabilità penale e civile nei casi previsti dalla normativa.

A tal fine, vengono fornite **informazioni ed istruzioni** alle quali attenersi per l'effettuazione dei trattamenti assegnati.

Relativamente agli **aspetti generali** delle attività di trattamento:

- trattare i dati personali, in base all'art. 5 del GPDR, in modo lecito, corretto e trasparente, assicurando che siano:
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità ("limitazione della finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati"); limitare attentamente i trattamenti alle sole necessità funzionali ai propri compiti da assolvere, rispettando le direttive del Delegato del Titolare;
- esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
- conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");

4 Dati personali particolari.
5 Dati personali giudiziari.
6 Abbreviazioni utilizzabili per la descrizione dei trattamenti principali:
- CREAZIONE - crea ed organizza l'archivio, raccoglie, registra ed inserisce nuovi dati;
- MODIFICA - modifica, estrae, elabora e cancella i dati;
- LETTURA - seleziona, raffronta e consulta i dati;
- COMUNICAZIONE - diffonde e comunica l'informazione;
- ARCHIVIAZIONE - archivia i dati;
- ELABORAZIONE - elabora e conserva i dati in formato digitale;
- TUTTI - effettua tutti i trattamenti previsti dal Delegato del Titolare.

- adeguatamente protetti da trattamenti non autorizzati o illeciti e da perdite, distruzioni o danni accidentali ("integrità e riservatezza");

- nell'ambito dello svolgimento delle Sue mansioni, qualora si verificasse l'esigenza di modificare trattamenti esistenti o introdurre nuovi trattamenti non compresi nel Suo profilo di autorizzazione, informare prontamente il Responsabile del Suo Ufficio; qualora ne ricorrano le condizioni, Le sarà rilasciata esplicita autorizzazione, da parte del Delegato del Titolare, per procedere con le modifiche dei trattamenti in corso e/o con l'avvio dei nuovi trattamenti;
- recepire le indicazioni sui trattamenti, da parte del Delegato del Titolare, anche partecipando a percorsi formativi, quando previsti;
- controllare e custodire con diligenza, durante lo svolgimento delle operazioni di trattamento, gli atti, i documenti e i supporti informatici di memorizzazione contenenti dati personali, per evitarne la visione dei dati, l'acquisizione e l'utilizzo non autorizzato da parte di terzi;
- non conservare/duplicare/comunicare i dati personali, di cui si è venuti a conoscenza durante le operazioni di trattamento, dopo la revoca esplicita dell'autorizzazione o dopo la cessazione del rapporto di lavoro;
- non comunicare/diffondere i dati personali all'esterno dell'Amministrazione senza preventiva autorizzazione del Delegato del Titolare; il divieto permane anche dopo la cessazione della presente autorizzazione e/o del rapporto di lavoro; la trasmissione di dati all'interno dell'Amministrazione è consentita solo per i compiti ed i fini stabiliti dal Delegato del Titolare e agendo sotto la sua diretta autorità;
- non fornire per telefono dati e informazioni relativi alla salute, qualora non si abbia certezza dell'identità del destinatario;
- rispettare ed applicare le norme di sicurezza per la protezione dei dati personali;
- segnalare, al Delegato del Titolare, eventuali circostanze che richiedano un necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- informare tempestivamente il Delegato del Titolare di ogni questione di rilievo, in relazione ai trattamenti effettuati e alle eventuali richieste pervenute dagli interessati;
- informare immediatamente il Delegato del Titolare nel caso in cui si constati o si sospetti un disguido o un incidente che abbia messo o possa mettere a repentaglio la sicurezza dei dati trattati;
- garantire agli interessati l'esercizio dei diritti sui propri dati secondo quanto previsto dal GDPR (diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, etc.);
- in caso di allontanamento dalla propria postazione di lavoro, adottare tutte le cautele necessarie atte ad evitare l'accesso, da parte di terzi non autorizzati, ai dati personali trattati sia in formato elettronico che cartaceo;
- senza previa autorizzazione del Responsabile del Suo Ufficio, non effettuare in alcun modo, di propria iniziativa, collegamenti di dispositivi mobili personali alla rete dati e/o ai PC dell'Ente;
- senza previa autorizzazione del Responsabile del Suo Ufficio, non trasferire in alcun modo, di propria iniziativa, materiale in formato elettronico o cartaceo, contenente dati personali ed afferenti l'attività lavorativa svolta, in luoghi esterni all'ufficio;
    - nel caso di lavoro agile, seguire le raccomandazioni fornite dal Titolare relativamente alle Raccomandazioni di sicurezza nell'utilizzo di informazioni e strumenti tecnologici
- fornire al Delegato del Titolare, a semplice richiesta o secondo le modalità indicate da questo, tutte le informazioni relative all'attività svolta, al fine di consentirgli un'adeguata azione di controllo;

Relativamente alle **misure di sicurezza** da adottare per ottemperare alle prescrizioni di cui al precedente paragrafo, fermo restando quanto previsto dal DISCIPLINARE SULL'USO DELLE RISORSE I.C.T. (information and communication technology) Approvato con D.G. 606 del 30/12/2009, si riportano di seguito alcuni aspetti di dettaglio**:**

- **Archiviazione dati**
  - non archiviare dati personali direttamente sul PC;
  - non utilizzare supporti e/o servizi online personali di memorizzazione non forniti dalla struttura preposte ai sistemi informativi;
  - non lasciare chiavette USB, Hard Disk esterni o altri supporti di memorizzazione a disposizione di estranei; riporre i supporti di memorizzazione in modo ordinato negli appositi contenitori e chiudere a chiave i classificatori e gli armadi dove sono custoditi;
  - nel caso di supporti di memorizzazione già utilizzati per il trattamento di dati relativi alla salute, procedere al loro riutilizzo solo se le informazioni precedentemente contenutevi non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti;
  - evitare di gestire le stesse informazioni su più archivi (ove non sia necessario) e, nel caso, curarne l'aggiornamento in modo organico;
  - conservare i dati relativi alla salute in armadi chiusi e ad accesso controllato o in file protetti da password;

- **Codici di accesso / Credenziali**
  - accedere al sistema per mezzo di credenziali di autenticazione; le credenziali di autenticazione più comuni consistono in un codice identificativo (user id o username) per l'identificazione della Persona autorizzata e una parola chiave (password) conosciuta solo dalla Persona autorizzata;
  - utilizzare password robuste con, qualora il sistema lo permetta, lunghezza minima di otto caratteri, lettere maiuscole, lettere minuscole, numeri e caratteri speciali (ad es., simboli di punteggiatura);
  - evitare di creare password con elementi o notizie facilmente riconducibili alla propria persona;
  - nel caso di password assegnata dall'amministratore, modificarla al primo utilizzo e ogni volta che viene richiesto dal sistema o nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza;
  - qualora il sistema non renda obbligatorio la modifica periodica della password, provvedere autonomamente a tale variazione sulla base delle indicazioni fornite dalla struttura preposta ai sistemi informativi;
  - adottare particolari cautele per assicurare la segretezza delle password, evitando ad esempio di essere osservati durante la digitazione e conservando i riferimenti in luoghi non accessibili a terzi;
  - per l'accesso alle banche dati telematiche, utilizzare sempre i propri codici di accesso personali, per consentire sempre la corretta individuazione dell'autore del trattamento, evitando di operare su terminali altrui e/o lasciare aperta la sessione di lavoro con i propri codici di accesso inseriti;

- **Gestione PC**
  - bloccare la sessione del PC ogni volta che ci si allontani dalla postazione di lavoro, sia per un tempo breve sia per un tempo più lungo, dovuto, ad esempio, ad una riunione, alla pausa pranzo o ad una missione fuori dalla sede di lavoro;
  - spegnere il PC alla fine della giornata lavorativa; nel caso in cui fosse necessario mantenere acceso il PC, assicurarsi di aver bloccato la sessione del PC;
  - non alterare in alcun modo la configurazione software del proprio PC, evitando in particolare di installare qualsiasi software non autorizzato dall'Amministrazione e di modificare/disattivare le impostazioni dell'antivirus;
  - qualora si dovessero riscontrare malfunzionamenti tecnici o anomalie nell'utilizzo del PC, segnalare al più presto tali eventi alla struttura preposta ai sistemi informativi;

- **Rete dati e posta elettronica**

- utilizzare la rete dati di Comune di Lamezia Terme solo per fini espressamente autorizzati;
- tenere un comportamento corretto durante la navigazione in Internet, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete;
- prestare la massima cura e attenzione nell'invio di informazioni attraverso i sistemi di comunicazione elettronica, controllando accuratamente l'indirizzo dei destinatari ed essendo consapevoli del rischio che possano essere rese disponibili al pubblico;
- non trasmettere via "e-mail standard" dati particolari o dati relativi a condanne penali o reati; i dati particolari riguardano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici identificativi, la salute, la vita sessuale, l'orientamento sessuale); nel caso in cui per ragioni d'ufficio sia strettamente necessaria tale forma di trasmissione, occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche; in particolare, si raccomanda il ricorso all'uso di tecniche di cifratura dei messaggi (file protetti da password, etc.);
- evitare di aprire o fare il download di documenti ricevuti di cui non sia certa la provenienza; nel dubbio consultare la struttura preposta ai sistemi informativi;

- **Trattamenti cartacei**
  - garantire sempre la corretta custodia dei documenti; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altre Persone autorizzate addette al medesimo trattamento; i documenti non possono essere riprodotti o fotocopiati, se non per esigenze connesse alle finalità del trattamento; i documenti non devono essere consultati da persone non autorizzate al trattamento;
  - conservare i documenti o gli atti, che contengono dati particolari e/o giudiziari, in archivi ad accesso controllato, come ad es. armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di personale preposto;
  - restituire tempestivamente la documentazione prelevata dagli archivi, al termine delle operazioni di trattamento;
  - in caso di utilizzo di stampanti, fotocopiatrici o fax, condivisi da vari utenti e collocati al di fuori dei locali ove è posta la propria postazione di lavoro, raccogliere e custodire immediatamente, con le modalità sopra descritte, tutte le stampe prodotte;
  - distruggere opportunamente le copie cartacee non più utili di documenti contenenti dati personali, evitando di gettarli via così come sono;
  - adottare misure che siano idonee a limitare la conoscenza dei dati particolari e/o giudiziari qualora essi siano presenti nei flussi documentali dell'Amministrazione, garantendo il rispetto della riservatezza dei dati degli interessati.

- **Rapporti di front-office:**
  - rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello (cd. Front-office) deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
  - identificazione dell'interessato: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere (si pensi a soggetti stranieri ovvero a dati identificativi che possono generare dubbi sulla correttezza della registrazione) ovvero con riferimento alla personalità della prestazione richiesta: può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- controllo dell'esattezza del dato: fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbe creare problemi nella gestione dell'anagrafica e nel proseguo del processo;
- obbligo di riservatezza e segretezza: l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;
- Cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:
- controllo dell'identità del richiedente: nel caso di richieste di comunicazione di dati (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti a mezzo intervista guidata; in altri casi, può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);
- verifica dell'esattezza dei dati comunicati: nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione all'esattezza del dato che viene comunicato, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor;

- **<u>Istruzioni per l'uso degli strumenti del trattamento - Telefono</u>**

Nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

- chiedere l'identità del chiamante e la motivazione della richiesta;
- richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
- verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante (ad esempio caserma dei carabinieri, servizi pubblici e di PS, …);
- procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;

- **<u>Istruzioni per l'uso degli strumenti del trattamento - FAX</u>**

Nell'utilizzare questo strumento occorre prestare attenzione a:

- digitare correttamente il numero di telefono, cui inviare la comunicazione;
- controllare l'esattezza del numero digitato prima di inviare il documento;
- verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli contemporaneamente;
- attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
- qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
- in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;

- **<u>Istruzioni per l'uso degli strumenti del trattamento – SCANNER</u>**

I soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;

Resta inteso che la presente designazione avrà la medesima durata del Suo rapporto con Comune di Lamezia Terme e che, successivamente alla cessazione di tale rapporto, Lei non sarà più autorizzato ad effettuare alcun tipo di trattamento sui dati.

Lamezia Terme, li _____

Il Responsabile del Trattamento delegato dal Titolare

Letto firmato e sottoscritto per presa visione La persona autorizzata

NOTE PER LA COMPILAZIONE DELLA TABELLA DEI TRATTAMENTI AUTORIZZATI

- **DP** - Indicare con "X" se si prevede l'accesso a dati personali particolari (relativi all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza sindacale, ai dati genetici, ai dati biometrici identificativi, alla salute, alla vita sessuale, all'orientamento sessuale).
- **DG** - Indicare con "X" se si prevede l'accesso a dati personali giudiziari (relativi a condanne penali e reati).
- **Trattamenti** - Descrivere i trattamenti autorizzati. E' possibile fare riferimento anche ai seguenti trattamenti predefiniti, riportandone il nome indicato in lettere maiuscole:

– *CREAZIONE* - crea ed organizza l'archivio, raccoglie, registra ed inserisce nuovi dati;
– *MODIFICA* - modifica, estrae, elabora e cancella i dati;
– *LETTURA* - seleziona, raffronta e consulta i dati;
– *COMUNICAZIONE* - diffonde e comunica l'informazione;
– *ARCHIVIAZIONE* - archivia i dati;
– *ELABORAZIONE* - elabora e conserva i dati in formato digitale;
– *TUTTI* - effettua tutti i trattamenti previsti dal Delegato del Titolare.

- **Compiti** - Compiti lavorativi che necessitano dei trattamenti indicati.
- **Revoca** - Eventuale data di revoca della designazione rispetto ai trattamenti indicati.

Modello di designazione degli amministratori di sistema (interni)

Lettera di designazione ad "Amministratore di Sistema"

ai sensi del "Provvedimento" del Garante per la protezione dei dati personali del 27 novembre 2008

Oggetto: **Designazione ad "Amministratore di Sistema"**

Al Sig._____C.F._____nato a_____il _____, matricola_____qualifica_____in forza presso l'Ufficio / Sezione / Settore

PREMESSO

- Che il Comune di Lamezia Terme, in qualità di Titolare del Trattamento, ha delegato i compiti e funzioni di cui all'art. 2, comma 2 del Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, a ciascun Responsabile di Settore o Ufficio di diretta collaborazione, quali "Responsabili del Trattamento" (di seguito anche "Delegati del Titolare"), ognuno per le attività di trattamento dei dati personali effettuate nell'ambito dell'articolazione amministrativa di cui sono responsabili;
- il rapporto di lavoro con Lei in essere e la Sua qualifica ed assegnazione organizzativa;
- che Lei ha già ricevuto, e sottoscritto per presa visione, la lettera di designazione quale "Persona autorizzata al trattamento dei dati personali";

CON LA PRESENTE

ad integrazione della suddetta lettera di designazione quale "Persona autorizzata al trattamento dei dati personali", avendo valutato che le prestazioni da Lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, la S.V. è designata quale "Amministratore di Sistema".

Tutte le operazioni di trattamento di dati personali saranno eseguite, con modalità e finalità decise dal Delegato del Titolare. Si riportano di seguito i sistemi ICT di cui viene chiesta la gestione e le relative funzioni attribuiteLe.

Utenza	**Sistema ICT da amministrare**	**Tipologia di amministrazione**			
		Rete[7]	**Sys**[8]	**DB**[9]	**Sw**[10]

7 Amministrazione di rete
8 Amministrazione di sistema
9 Amministrazione di data base - DBA
10 Amministrazione di sistema software complesso

Per effetto di tale designazione e delle funzioni conseguentemente attribuite, Lei si impegna a:

- accedere ai sistemi ICT nei limiti strettamente richiesti dall'espletamento delle Sue mansioni;
- eseguire gli accessi nel rispetto delle procedure di autenticazione a Lei già note, e di detenzione, custodia, segretezza e sicurezza delle relative credenziali di accesso;
- eseguire gli accessi nel rispetto delle misure di sicurezza organizzative, logiche e fisiche adottate dal Titolare del Trattamento;
- attenersi alle istruzioni operative impartite dal Titolare o suo Delegato;
- segnalare qualunque elemento che possa pregiudicare il corretto svolgimento delle Sue funzioni di Amministratore di Sistema e/o rendere necessarie ulteriori istruzioni;
- cooperare con il Delegato del Titolare per ogni verifica della rispondenza del Suo operato alle misure organizzative, tecniche e di sicurezza previste con riferimento ai dati personali trattati per conto e nell'interesse dell'ente;
- collaborare per l'attuazione delle eventuali ulteriori prescrizioni che saranno emanate dall'Autorità Garante per la Protezione dei Dati Personali in tema di amministratori di sistema;
- consentire il trattamento dei Suoi dati personali nei limiti e per le finalità previste dal citato provvedimento in data 27.11.2008 dell'Autorità Garante per la Protezione dei Dati Personali, incluso la registrazione e comunicazione di ogni dato di log, ogni comunicazione a terzi, nonché la divulgazione dei Suoi dati identificativi ai dipendenti dell'ente nell'ambito delle attività organizzative dello stesso.

Resta inteso e convenuto che:

- la presente designazione non configura alcuna variazione della Sua qualifica e delle Sue mansioni e del relativo trattamento economico e normativo del rapporto di lavoro con Lei in essere;
- la registrazione e comunicazione dei dati di log sarà eseguita al solo fine di ottemperare a quanto specificatamente prescritto al riguardo dal citato provvedimento in data 27.11.2008 dell'Autorità Garante per la Protezione dei Dati Personali e non costituisce alcuna forma di controllo a distanza, neanche indiretto, della Sua attività lavorativa;
- ogni eventuale variazione dell'ambito di operatività consentito dalle Sue mansioni e dal Suo profilo di autorizzazione all'accesso ai sistemi ICT non comporterà il venir meno degli effetti della presente designazione.

Le ricordiamo, che il provvedimento del Garante già citato, obbliga il Titolare del Trattamento alla "verifica" almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Distinti saluti

Lamezia Terme, li _____

Il Responsabile del Trattamento delegato dal Titolare

Letto firmato e sottoscritto per accettazione
L'amministratore di sistema

NOTE PER LA COMPILAZIONE DELLA TABELLA DEI SISTEMI ICT DA AMMINISTRARE

- **Tipologia di amministrazione** - Indicare con "X" la tipologia di amministrazione richiesta.
- **Sistema ICT da amministrare** - Si riporta un elenco di sistemi di esempio per ogni tipologia di amministrazione:

– *amministrazione di rete* - sonde IPS/IDS, proxy server, firewall e apparati di sicurezza perimetrale, dispositivi d'instradamento del traffico (router, switch), etc.

– *amministrazione di sistema* - sistemi Operativi, sistemi software di base, middleware, sistemi o infrastrutture di Backup, etc.

– *amministrazione di data base* - data base management systems, data warehouse systems, big data systems, etc.

– *amministrazione di sistemi software complessi* - sistema amministrativo centrale, sistema sanità, sistema turismo, etc.

- **Ambito di operatività e funzioni attribuite** - Si riporta un elenco di ambiti di operatività e funzioni di esempio per ogni tipologia di amministrazione:

– *amministrazione di rete* - gestione delle credenziali di accesso e delle configurazioni di sicurezza dei dispositivi di sicurezza e di rete; gestione e configurazione di apparati dedicati alla sicurezza di rete e al traffico telematico all'interno di una rete di telecomunicazione; effettuazione attività di manutenzione ordinaria e straordinaria sugli apparati di sicurezza e di rete; effettuazione di attività di salvataggio e ripristino dei dati e delle configurazioni; etc.

– *amministrazione di sistema* - gestione delle credenziali di accesso e delle configurazioni di sicurezza dei sistemi operativi, file system, middleware, infrastrutture; gestione e configurazione dei sistemi operativi; effettuazione attività di manutenzione ordinaria e straordinaria sui sistemi operativi; effettuazione di attività di salvataggio e ripristino dei dati e delle configurazioni; etc.

– *amministrazione di data base* - gestione delle credenziali di accesso e delle configurazioni di sicurezza dei Data Base; gestione e configurazione dei Data Base; effettuazione attività di manutenzione ordinaria e straordinaria sui Data Base; effettuazione di attività di salvataggio e ripristino dei dati e delle configurazioni; erogazione servizio di supporto di 3° livello; supporto attraverso analisi specifiche; etc.

– *amministrazione di sistemi software complessi* - gestione delle credenziali di accesso e delle configurazioni di sicurezza applicativa; effettuazione attività di manutenzione ordinaria e straordinaria sui sistemi software complessi; applicazione patch o pacchetti software concernenti le applicazioni gestite; effettuazione di attività di salvataggio e ripristino dei dati e delle configurazioni; erogazione servizio di supporto di 3° livello; supporto attraverso analisi specifiche, etc.