COMUNE DI OTTANA
PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO A TUTELA DEI DATI PERSONALI

(Approvato con deliberazione di Consiglio Comunale n. 32 del 27/07/2023)

Sommario

PREMESSA

Il 25 maggio 2018 è divenuto ufficialmente operativo il nuovo Regolamento generale in materia di Protezione dei Dati personali. Il GDPR, acronimo di "General Data Protection Regulation" va ad abrogare, dopo oltre un ventennio, la cosiddetta direttiva madre n. 95/46/C, che, fino ad oggi, costituiva il quadro normativo di riferimento a livello europeo. Il nuovo Regolamento costituisce, insieme alla Direttiva (UE) n. 2016/680, il "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea. Il Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 fa riferimento a dati concernenti persone identificate o identificabili in possesso di vari soggetti e quindi anche della Pubblica amministrazione utilizzabili per le proprie finalità istituzionali. Dati che devono essere trattati nei limiti delle funzioni dell'ente, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.

Il nuovo apparato normativo si regge su di un nuovo principio di fondamentale importanza: la responsabilizzazione, ovvero il principio di accountability (nell'accezione inglese).

Tale concetto rappresenta un'assoluta novità nel campo della protezione dei dati personali, in quanto il titolare del trattamento, oltre ad avere l'esclusiva competenza per il rispetto dei principi e delle regole previste dal GDPR, deve anche essere in grado di comprovarne il corretto adempimento.

Ai titolari, altresì, viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri indicati dal regolamento.

Come specifica chiaramente l'art. 25 del GDPR, uno di quei criteri è sicuramente rappresentato dall'espressione anglofona "*data protection by default and by design*" ossia dalla necessità di configurare il trattamento prevedendo dall'inizio, ovvero fin dalla fase di progettazione, le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Spetta dunque al titolare mettere in atto una serie di misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.

Tra le nuove attività previste dal GDPR, riguardo agli obblighi dei titolari, saranno fondamentali quelle relative alla valutazione del rischio inerente il trattamento. Quest'ultimo è da intendersi come rischio da impatti negativi sulle libertà e sui diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per diminuirne l'impatto.

Una lettura organica e sistematica del Regolamento europeo consente di affermare che, data l'importanza della normativa e di ciò che essa mira a proteggere, la migliore risposta in termini di cambiamento organizzativo sia quella di realizzare un complessivo "Modello organizzativo e di gestione" per la protezione dei dati personali, considerando come tale un complesso di attività organizzativa, di ruoli, di azioni organizzative, di sistemi mirato al fine dell'applicazione "ordinata" e completa, nell'azione amministrativa dell'Ente, della normativa sui trattamenti di dati personali. Tale logica di costruzione di un Modello ad hoc è, peraltro, simile a quella risultante, in materia di prevenzione della corruzione.

L'adeguamento al Regolamento UE 2016/679 impone al Titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, l'approvando Modello organizzativo individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche, logiche, logistiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Al fine di garantire la migliore e più puntuale attuazione del principio di accountability, il presente modello organizzativo contiene disposizioni regolamentari minime la cui concreta attuazione è demandata all'organizzazione del personale operante all'interno dell'Ente, nelle sue articolazioni gerarchiche.

E' ammesso ed anzi incoraggiato l'utilizzo di modulistica differente rispetto a quella allegata al presente modello a condizione che essa ne rispetti i criteri e le regole generali.

Il presente modello organizzativo sarà sottoposto a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

PARTE I - NORME E PRINCIPI GENERALI

Questa Amministrazione assicura che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza. In attuazione del suddetto principio il Comune assicura che, nello svolgimento dei compiti e funzioni istituzionali, i dati personali siano trattati nel rispetto della legislazione vigente oltre che dei seguenti principi:

a) «liceità, correttezza e trasparenza»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) «limitazione delle finalità»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, prf. 1 del RGDP, considerato incompatibile con le finalità iniziali;

c) «minimizzazione dei dati»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «necessità»: è ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità;

e) «esattezza»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

f) «limitazione della conservazione»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, prf. 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato;

g) «integrità e riservatezza»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

h) «responsabilizzazione»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo.

SENSIBILIZZAZIONE E FORMAZIONE

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Comune sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, questa Amministrazione riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale nonché quella diretta a tutti coloro che hanno rapporti con il Comune.

Per garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio, è data ad ogni dipendente una specifica comunicazione, con apposita clausola inserita nel

contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente Modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie.

Il Comune organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Comune.

La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

TRATTAMENTO DEI DATI PERSONALI

Il Comune tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali, quali identificate da disposizioni di legge, statutarie e regolamentari, e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo.

Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati ed autorizzati secondo quanto previsto infra nel presente documento. Non è consentito il trattamento da parte di persone non puntualmente autorizzate ed istruite in tal senso.

Al fine di garantire la correttezza delle operazioni di trattamento il Comune provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti svolti, finalizzata alla compilazione ed aggiornamento del Registro delle attività di trattamento di cui al GDPR.

Tipologie di dati trattati

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali il Comune, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati personali, quali definiti all'articolo 4, paragrafo 1 del GDPR;
- categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR (c.d. dati sensibili);
- categorie particolari di dati personali di cui all'articolo 2-septies del D.Lgs. 196/2003 (c.d. dati super-sensibili);
- dati personali relativi a condanne penali e reati di cui all'articolo 10 del GDPR (c.d. dati giudiziari)

Finalità del trattamento

Il Comune effettua periodicamente una ricognizione delle finalità che impongono o consentono il trattamento dei dati personali, anche sensibili (e super-sensibili) e giudiziari.

In sede di prima stesura del presente documento, viene predisposto apposito elenco (a carattere esemplificativo e non esaustivo) contenente le principali finalità del trattamento, allegato sotto la lettera "1".

CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizione normative che lo vietino, il Comune favorisce la circolazione all'interno dei propri uffici dei dati personali dei cittadini il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del GDPR.

La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti.

Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati dagli articoli 9 e 10 del GDPR.

COORDINAMENTO DI NORME

Questa Amministrazione intende perseguire l'obiettivo di assicurare le forme più estese di accessibilità e trasparenza sul proprio operato ad opera dei cittadini, nelle varie forme in cui il diritto di accesso è riconosciuto, quali (a titolo esemplificativo) quella prevista dal TUEL (D.Lgs. 267/2000) negli articoli 10 e 43, quella prevista dalla Legge 241/90 e quella prevista dal D.Lgs. 33/2013.

A tale proposito - fermo restando che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato e la relativa tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione restano disciplinati dalla normativa di settore – gli Uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto (eventualmente, in caso di accesso) controinteressato.

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigente, l'Ufficio, nel dare riscontro alle richieste di accesso ovvero nel pubblicare i provvedimenti, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei «dati personali» in esso presenti, laddove l'esigenza informativa, alla base dell'accesso o della trasparenza e pubblicazione, possa essere raggiunta senza implicare il trattamento dei dati personali.

PARTE II - PROFILO ORGANIZZATIVO

PROFILO STRUTTURALE

La prima risposta organizzativa è l'individuazione di una struttura organizzativa per la protezione dei dati personali, che, ovviamente, si sovrapponga, in gran parte, all'attuale struttura amministrativa dell'Ente, integrandosi con essa. la creazione di tale struttura, comporta tre azioni principali:

• il disegno di struttura (organigramma) per la Privacy;
• la definizione dei ruoli;
• l'individuazione dei soggetti "abilitati" dall'Ente a trattare i dati personali.

Conseguente, alla costruzione, sarà quindi necessario adeguare le competenze mediante la formazione e informazione dei soggetti, abilitando concretamente i soggetti stessi.

IL TITOLARE DEL TRATTAMENTO

L'art. 4 n. 7 del GDPR precisa che il titolare del trattamento (interpretando la norma rispetto all'Ente locale) è "*l'autorità pubblica*" che "*determina le finalità e i mezzi del trattamento di dati personali*".

Il concetto di Titolare del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:

a) determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);
b) mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. accountability) (art. 24);
c) garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
d) individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
e) agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
f) designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
g) istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
h) effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
i) comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
l) ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
m) rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
o) rispondere delle violazioni amministrative ai sensi del GDPR (art. 83)

Alla luce del testo normativo e delle interpretazioni correnti, si ritiene che titolare sia l'Ente locale nel suo complesso in quanto la legislazione nazionale gli ha affidato il compito di raccogliere e trattare certi

dati personali. Tuttavia, in concreto, esso manifesta la propria volontà attraverso coloro a cui è attribuito il potere di decidere per l'Ente, nell'ambito delle suddivisioni di ruolo nascenti dal diritto amministrativo.

Le competenze e le responsabilità quali delineate dal GDPR e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi del Comune in relazione alle funzioni agli stessi assegnati dal D.Lgs. n. 267/2000 e dallo statuto comunale. Tale ripartizione è così intesa da questa Amministrazione:

A. al Consiglio comunale sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;
B. all'organo esecutivo (Giunta comunale) sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del Consiglio, con particolare riferimento agli atti e attività a contenuto organizzativo e di indirizzo;
C. all'organo di vertice (Sindaco) competono le nomine e le designazioni rilevanti in materia di protezione dei dati personali, con riferimento in particolare al Responsabile della protezione dei dati, ai soggetti designati con funzioni di coordinamento (Dirigenti e Responsabili di posizione organizzativa), al Segretario / Direttore generale;
D. ai Dirigenti e Responsabili di posizione organizzativa, secondo l'ambito di competenza, spettano i seguenti compiti (con elencazione meramente esemplificativa):
a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
b) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c) adottare soluzioni di privacy by design e by default;
d) contribuire al costante aggiornamento del registro delle attività di trattamento;
e) garantire la corretta informazione e l'esercizio dei diritti degli interessati;
f) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
g) disporre l'adozione dei provvedimenti imposti dal Garante;
h) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
i) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
l) garantire al Responsabile della protezione dei dati personali ed al personale (eventualmente) designato Amministratore di sistema i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
m) la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
n) consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1, lett b), nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
o) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;
p) individuare i responsabili (esterni) ed i contitolari del trattamento fornendo le necessarie indicazioni.

AUTORIZZATO AL TRATTAMENTO

Il GDPR non prevede espressamente la figura degli "incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'articolo 29, rubricato "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", il quale stabilisce che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";

Il Codice privacy, all'articolo 2-quaterdecies prevede che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

Il GDPR e la normativa nazionale di adeguamento consentono dunque di mantenere le funzioni ed i compiti assegnati a figure interne all'Ente che, ai sensi del Codice nel testo previgente all'adeguamento al GDPR, ma non anche ai sensi del GDPR, potevano essere definiti come "incaricati".

Il personale operante (a qualunque titolo ed a qualunque livello) all'interno del Comune è conseguentemente autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al presente modello organizzativo.

Spetta ai Dirigenti / Responsabili di P.O. identificare e designare - sulla base delle indicazioni contenute nell'Allegato "2" al presente documento - per iscritto ed in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, che operano sotto la diretta autorità del Titolare ed attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni e controllando costantemente che le persone fisiche designate, delegate e autorizzate al trattamento dei dati effettuino le operazioni di trattamento:

- in attuazione del principio di «liceità, correttezza e trasparenza»;
- in attuazione del principio di «minimizzazione dei dati»;
- in attuazione del principio di «limitazione della finalità»;
- in attuazione del principio di «esattezza»;
- in attuazione del principio di «limitazione della conservazione»;
- in attuazione del principio di «integrità e riservatezza»;
- in attuazione del principio di «liceità, correttezza e trasparenza»

DIRIGENTI / RESPONSABILI DI POSIZIONE ORGANIZZATIVA (P.O.) - DESIGNATI AL TRATTAMENTO

In attuazione del D.Lgs. n. 196/2003, nel testo previgente all'adeguamento al GDPR, i Dirigenti / Responsabili di Posizione organizzativa (P.O.) sono stati nominati, come da nomine in atti, responsabili interni del trattamento dei dati per i trattamenti rientranti nella competenza di ciascuno di essi.

L'articolo 28 del GDPR ha definito il Responsabile del trattamento come il soggetto che effettua il trattamento "*per conto del titolare*".

In forza del rapporto di immedesimazione organica che intercorre tra i Dirigenti / Responsabili di Posizione organizzativa (P.O.) ed il Titolare, non risulta configurabile un rapporto di rappresentanza "*per conto del titolare*";

In considerazione dell'entrata in vigore della nuova normativa del GDPR e della modificata definizione di Responsabile del trattamento, si rende necessario procedere all'adeguamento degli atti di

nomina dei Dirigenti /Responsabili di Posizione organizzativa (P.O.), al fine di attribuire ai medesimi, in qualità di soggetti appositamente designati, specifici funzioni e compiti connessi al trattamento dei dati personali.

Conformemente alle disposizioni del GDPR e del Codice della privacy nel suo testo vigente, il Titolare ed il Responsabile del trattamento possono quindi designare, sotto la propria responsabilità ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati.

Questa Amministrazione ritiene dunque che i Dirigenti / Responsabili di Posizione organizzativa (P.O.) debbano conseguentemente essere autorizzati al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al paragrafo che precede.

Considerato che ai Dirigenti / Responsabili di P.O. spettano l'adozione degli atti e provvedimenti amministrativi, compresi tutti gli atti che impegnano l'amministrazione verso l'esterno, nonché la gestione finanziaria, tecnica ed amministrativa mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo e che essi sono responsabili, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui sono preposti, appare opportuno attribuire loro specifici compiti e funzioni spettanti al Titolare, ferma restando l'imputazione della responsabilità conseguente al trattamento in capo al Titolare medesimo.

Spetta al Sindaco identificare e designare i Dirigenti / Responsabili di posizione organizzativa (P.O.) cui assegnare lo svolgimento di specifici compiti e funzioni sulla base delle indicazioni contenute nell'Allegato "3" al presente documento.

SEGRETARIO COMUNALE / DIRETTORE GENERALE - DESIGNATO AL TRATTAMENTO

In attuazione del D.Lgs. n. 196/2003, nel testo previgente all'adeguamento al GDPR, il Segretario comunale / Direttore generale è stato nominato, come da nomina in atti, responsabile interno del trattamento dei dati per i trattamenti rientranti nella sua competenza.

L'articolo 28 del GDPR ha definito il Responsabile del trattamento come il soggetto che effettua il trattamento "*per conto del titolare*".

Considerato il ruolo e le funzioni del Segretario comunale quali definiti nell'articolo 97 del D.Lgs. 18 agosto 2000 n. 267 (TUEL), non risulta configurabile un rapporto di rappresentanza "per conto del titolare".

In considerazione dell'entrata in vigore della nuova normativa del GDPR e della modificata definizione di Responsabile del trattamento, si rende necessario procedere all'adeguamento degli atti di nomina dei Dirigenti /Responsabili di Posizione organizzativa (P.O.), al fine di attribuire ai medesimi, in qualità di soggetti appositamente designati, specifici funzioni e compiti connessi al trattamento dei dati personali.

Conformemente alle disposizioni del GDPR e del Codice della privacy nel suo testo vigente, il Titolare ed il Responsabile del trattamento possono quindi designare, sotto la propria responsabilità ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati.

Questa Amministrazione ritiene dunque che il Segretario comunale / Direttore generale debba conseguentemente essere autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità ai paragrafi che precedono.

Spetta al Sindaco identificare e designare il Segretario comunale / Direttore generale cui assegnare lo svolgimento di specifici compiti e funzioni sulla base delle indicazioni contenute negli Allegati "4" al presente modello organizzativo, in qualità anche di referente.

Ai sensi dell'articolo 38 del GDPR, infatti il Titolare ha l'obbligo di assicurarsi che "*il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la*

protezione dei dati personali"; il Titolare inoltre sostiene "*il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".

Si ravvisa dunque la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati - di individuare uno o più dipendenti interni all'Ente cui assegnare il compito di "Referente" al fine di supportare l'attività del Responsabile della Protezione dei dati personali (RPD o DPO), nelle seguenti attività:

a) informazione e consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori best practice in materia di analisi e valutazione dei rischi.

b) sorveglianza dell'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei software e della relativa documentazione tecnica;

d) cooperare con l'Autorità di controllo e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva prevista dall'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.

Il Referente è tenuto al segreto od alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al RPD ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.

Ove i compiti assegnati al Referente vengano svolti in modo collettivo da parte di un team, dovrà essere designato un soggetto coordinatore.

Spetta al Segretario comunale identificare e designare il Referente cui assegnare lo svolgimento di specifici compiti e funzioni in caso di delega.

AMMINISTRATORE DEL SISTEMA INFORMATICO

Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" come modificato con successivo provvedimento datato 25/06/2009, il Comune si avvale di un amministratore del sistema informatico a garanzia che il sistema informatico di questo Ente sia strutturato e gestito in modo da consentire l'attuazione delle misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.

L'amministratore del sistema deve essere in possesso di titolo di studio specifico in informatica almeno di scuola media di secondo grado o laurea triennale e di comprovate conoscenze specialistiche tecniche e giuridiche in materia di sicurezza degli strumenti e dei programmi informatici per la protezione dei dati personali nonché della capacità di assolvere i compiti di competenza.

Amministratore del sistema informatico può essere designato un dipendente comunale a tempo indeterminato inquadrato almeno nella categoria "C" ovvero, nel caso di mancanza di un dipendente, un soggetto esterno, persona fisica o giuridica.

Nell'atto ovvero nel contratto di servizio con cui è designato l'Amministratore di sistema devono essere riportati, altresì, tutti gli adempimenti – con tutto ciò che essi comportano sia sul piano delle

procedure amministrative, che dell'organizzazione, che dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali – imposti dalle fonti di diritto europee e nazionali, dal "Gruppo di Lavoro europeo ex art. 29", dal Garante della Privacy, dalle disposizioni regolamentari e dalle direttive emanate dal Titolare del trattamento e dal Responsabile della protezione dei dati, nonché per conformarsi alla disciplina del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82/2004 e ss.mm.ii., in particolare la cura dei seguenti adempimenti:

a) gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;

b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;

c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema; impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per gli Incaricati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzate;

d) verificare costantemente che il Comune abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo senza indugio agli adeguamenti eventualmente necessari, redigendo entro il 30 settembre di ogni anno una apposita relazione da inviare al Sindaco, al Segretario ed al Responsabile per la protezione dei dati in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure;

e) suggerire al Comune l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati, atte a che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

Più specificamente, l'Amministratore di sistema dovrà svolgere le funzioni previste in apposito Disciplinare tecnico sulla base di quanto contenuto nell'Allegato "5".

All'Amministratore del sistema informatico è:

a) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Responsabili del trattamento a conoscere i dati personali oggetto di trattamento;

b) obbligato a dare tempestiva comunicazione al Sindaco ed ai Responsabili del trattamento interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;

c) obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.

Il Responsabile della protezione dei dati procederà periodicamente alla verifica delle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

IL CONTITOLARE DEL TRATTAMENTO

In base alla previsione contenuta nell'articolo 26 del GDPR "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di*

cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati".

In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.

Spetta ai Dirigenti / Responsabili di P.O. identificare gli eventuali contitolari di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni per il trattamento dei dati avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai contitolari l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni.

Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.

I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali. E' tuttavia ammessa una diversa ripartizione "Interna" del profilo di responsabilità, da valutarsi caso per caso.

Il contenuto essenziale dell'accordo di Contitolarità è messo a disposizione degli interessati nella sezione Trasparenza del Portale di ciascuno dei Contitolari.

IL RESPONSABILE DEL TRATTAMENTO

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.

L'esistenza di un Responsabile del trattamento dipende da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità - o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.

A norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".

Per poter agire come Responsabile del trattamento occorrono quindi due requisiti: essere una persona giuridica distinta dal Titolare ed elaborare i dati personali per conto di quest'ultimo.

La liceità dell'attività di trattamento dei dati da parte del Responsabile è determinata dal mandato ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile diventa (con)Titolare.

Si deve tuttavia prendere atto del fatto che esistano situazioni in cui la relazione tra l'Amministrazione comunale ed un altro soggetto, pubblico o privato possa generare dei dubbi in merito alla corretta qualificazione del ruolo soggettivo rivestito (Titolare o Responsabile). Con riferimento a tali fattispecie, questo Ente adotta il criterio della valutazione delle circostanze di fatto, suggerito dal Gruppo ex art. 29 nel Parere 1-2010 (WP 169).

Il paragrafo 3 dell'articolo 28 del GDPR prevede che "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*"; il paragrafo 9, da ultimo, prevede che "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*".

Spetta ai Dirigenti / Responsabili di P.O. identificare i responsabili e gli eventuali sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati - sulla base delle indicazioni contenute nell'Allegato "06" al presente modello organizzativo - avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai responsabili e dagli eventuali sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi, risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni.

Il Dirigente / Responsabile di P.O. competente per materia in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.

La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

Il Comune si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD o DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.

Il Responsabile della protezione è designato con decreto del Sindaco non oltre sei mesi dalla data della sua proclamazione. Sino alla designazione del nuovo Responsabile della protezione dei dati si intende prorogata di diritto la designazione del Responsabile della protezione dei dati in carica al momento della predetta proclamazione. Tale proroga é valida anche a seguito della nomina di un Commissario che sostituisca tutti gli organi di governo dell'Ente, salvo che lo stesso Commissario non ritenga necessario designare un nuovo Responsabile della protezione dei dati ovvero sostituire il Responsabile in carica all'atto della sua nomina.

Responsabile della protezione dei dati può essere designato il Segretario Comunale o un Dirigente o un dipendente a tempo indeterminato di questo Comune inquadrato in una categoria non inferiore alla C) ovvero un soggetto esterno, persona fisica o soggetto giuridico.

L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del RPD.

I dati identificativi e di contatto del Responsabile della protezione dei dati sono pubblicati nel sito web istituzionale dell'Ente, rendendoli accessibili da un apposito link, comunicati all'Autorità di controllo, comunicati ai componenti degli organi di governo, a tutti i dirigenti e dipendenti comunali, ai componenti degli organi di controllo interni nonché sono inclusi in tutte le informative rese agli interessati ai sensi degli articoli 14 e 14 del GDPR.

I compiti e le funzioni demandate al Responsabile della protezione dei dati sono quelli indicati nella bozza di decreto di nomina di cui all'Allegato "07".

PARTE III - ADEMPIMENTI E PROCEDURE

MISURE PER LA SICUREZZA DEI DATI PERSONALI

La Giunta comunale, i Dirigenti / Responsabili di P.O. e l'Amministratore del sistema informatico provvedono, per quanto di rispettiva competenza, all'adozione ed alla dimostrazione di aver adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Ai sensi dell'articolo 30 del GDPR "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*"; la medesima norma individua il contenuto minimo di tale registro, specificando poi che esso è tenuto in forma scritta, anche in formato elettronico e dev'essere messo a disposizione dell'autorità di controllo.

La tenuta di siffatto registro si configura pertanto come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal GDPR e non soltanto come strumento operativo di mappatura dei trattamenti effettuati.

Un'altra grande differenza rispetto al D.lgs. 196/2003 è la modalità di mantenimento di tale documento. Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato.

E' intenzione del Comune adottare un sistema informatico che meglio possa consentire l'aggiornamento e l'accesso alle informazioni. Il sistema informatico dovrà rispettare il contenuto prescritto dal GDPR e dovrà tener conto delle prescrizioni impartite dal Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) nonché dal Garante per la protezione dei dati personali.

Una elaborazione cartacea del registro è sottoposta all'approvazione della Giunta comunale con cadenza almeno annuale mentre una sua copia informatica è posta in conservazione sostitutiva.

In ragione delle dimensioni, anche organizzative di questa Amministrazione, le operazioni tecniche connesse all'istituzione, alla compilazione ed all'aggiornamento delle informazioni contenute nel Registro sono demandate ad un fornitore di servizi software esterno, scelto nel rispetto della vigente normativa in materia di appalti pubblici, il quale presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Tale soggetto esterno sarà designato quale Responsabile del trattamento.

Spetta ai Dirigenti / Responsabili di P.O.:

- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ufficio, al fine di consentire la compilazione del registro;

- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati, da sottoporre all'approvazione del Titolare;
- contribuire alla tenuta del registro in relazione ai trattamenti della struttura organizzativa di competenza, fornendo le necessarie informazioni e valutazioni

Qualora l'Amministrazione decida di provvedere alla gestione ed aggiornamento del registro, senza avvalersi di un soggetto esterno, dovrà designare allo scopo un Dirigente / Responsabile di P.O. in modo da garantirne l'effettività.

Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamento è demandata alla figura del DPO.

Ai sensi dell'art. 39 del GDPR che disciplina infatti le prerogative del Responsabile della protezione dei dati personali si evince che tra le altre è tenuto a "*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*".

All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunge il principio di accountability che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della compliance normativa.

VALUTAZIONI DI IMPATTO SULLA PROTEZIONE DEI DATI

Nel caso in cui una tipologia di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

La valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi. Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo processo di DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del GDPR.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi. L'aggiornamento della valutazione d'impatto sulla protezione dei

dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità.

Il Dirigente / Responsabile di P.O. conduce quindi una prima fase di valutazione preliminare, il cui scopo è quello di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento sia conforme al GDPR e, in seconda battura, comprendere se quel trattamento debba essere sottoposto ad una valutazione DPIA. L'attività quindi si scompone di 3 sotto fasi:

a. descrizione del trattamento (le categorie di soggetti interessati dal trattamento, le finalità del trattamento, le categorie di dati oggetto del trattamento, le modalità di trattamento, il luogo di conservazione dei dati trattati, …) sulla scorta delle risultanze contenute nell'apposito registro;

b. valutazione della conformità (analisi della necessità e della proporzionalità del trattamento rispetto alle finalità; rispetto dei principi applicabili al trattamento di cui al capo II del GDPR; rispetto dei diritti degli interessati di cui al capo III del GDPR);

c. valutazione della obbligatorietà di condurre una DPIA;

Fermo restando quanto indicato dall'art. 35, paragrafo 3, del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del GDPR;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato, sentito il Responsabile della protezione dei dati e l'Amministratore del sistema informatico (se esistente), ritenga motivatamente che non possa presentare un rischio elevato; il Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato può, motivatamente, ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

La DPIA non è necessaria nei casi seguenti:

a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del GDPR;

b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è inoltre necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità di controllo o dal Responsabile della protezione dei dati personali e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni dell'Autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

Una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti. L'attività si scompone in ulteriori 4 sotto fasi:

a. raccolta delle informazioni per l'analisi dei rischi (informazioni presenti all'interno dei trattamenti, procedimenti coinvolti dal trattamento, finalità dei dati raccolti, flussi informativi, autorizzati all'accesso alle informazioni, asset model a sostegno dei trattamenti (applicativi, hardware, reti, ecc.). Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato)

b. valutazione dei rischi, di norma sviluppata nel classico concetto di valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromette un asset (informativo) (alcuni esempi sono gli impatti derivanti da una violazione della sicurezza fisica; da una violazione dei dati di identificazione o attinenti l'identità personale; perdite finanziarie o al patrimonio, perdite dovute a frodi; turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute, evento lesivo dei diritti umani inviolabili o dell'integrità della persona; conseguenze di tipo discriminatorio, perdite di autonomia);

c. valorizzazione delle contromisure e rischio residuo. L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile;

d. piano di trattamento dei rischi;

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

1) delle finalità specifiche, esplicite e legittime;
2) della liceità del trattamento;
3) dei dati adeguati, pertinenti e limitati a quanto necessario;
4) del periodo limitato di conservazione;
5) delle informazioni fornite agli interessati;
6) del diritto di accesso e portabilità dei dati;
7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
8) dei rapporti con i responsabili del trattamento;
9) delle garanzie per i trasferimenti internazionali di dati;
10) consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
e) l'acquisizione del parere del Responsabile della protezione dei dati personali

Assume quindi fondamentale importanza l'attività di formalizzazione dei risultati la quale consiste nel valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva.

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un documento finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR. Il documento deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

L'Ufficio può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato garantisce l'effettuazione della DPIA ed è responsabile della stessa, salvo che ne affidi l'esecuzione ad altro soggetto, anche esterno al Comune.

Il Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato deve consultarsi con il Responsabile della protezione dei dati personali anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato devono essere documentate nell'ambito della DPIA.

L'Ufficio deve consultare l'Autorità di controllo prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato (tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il GDPR, in particolare qualora l'Ufficio non abbia identificato o attenuato sufficientemente il rischio). L'Ufficio consulta l'Autorità di controllo anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo.

Salvo diversa disposizione dell'Autorità di controllo è bene che la comunicazione di richiesta di consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data.

L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

Il processo DPIA deve sempre prevedere un monitoraggio dei risultati raggiunti ed un conseguente e costante riesame al fine di garantire nel tempo la mitigazione dei rischi e la conformità al GDPR, anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno ed esterno, finalità del trattamento, strumenti utilizzati, organizzazione comunale, presenza di nuove minacce, ecc.).

Il Responsabile della protezione dei dati personali monitora lo svolgimento della DPIA. Può inoltre proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di

mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Eventuali Responsabili del trattamento collaborano e assistono l'Ufficio oltre che il Responsabile della protezione dei dati nella conduzione della DPIA fornendo ogni informazione necessaria.

L'Amministratore del sistema informatico (se designato) fornisce il necessario supporto al Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato per lo svolgimento della DPIA. Può inoltre proporre di condurre una DPIA in relazione ad uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Dal punto di vista operativo - considerata la complessità di un processo DPIA e relativa fase di analisi dei rischi – l'Ufficio deve adottare strumenti applicativi specializzati in grado di gestire tutte le fasi del processo ed in grado di riproporre la sua applicabilità nel tempo.

Un esempio di un software applicativo per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di CNIL (Autorità francese per la protezione dei dati). Il software, al quale ha aderito anche il garante Italiano, non costituisce un modello al quale fare sempre riferimento (si ricorda che è stato concepito soprattutto per le PMI), ma può offrire un focus sugli elementi principali di cui si compone la procedura di DPIA. Può quindi costituire un utile supporto metodologico e di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate.

Può servire inoltre per comprendere meglio quali possono essere i requisiti di base di un applicativo DPIA adeguato alla propria realtà procedendo quindi ad una software selection più mirata e consapevole.

E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

VIOLAZIONE DEI DATI PERSONALI

Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune (tale indicazione operativa pertanto si applica a tutti gli archivi/documenti cartacei ed a tutti i sistemi, anche informativi sui quali siano conservati i dati personali degli interessati, quali cittadini, dipendenti, fornitori, soggetti terzi, ecc.).

La segnalazione di un possibile Data Breach può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali ecc.) o dall'interno, da parte delle varie funzioni di settore durante il normale svolgimento dell'attività lavorativa (più frequentemente tali eventi vengono evidenziati da funzioni che svolgono attività di verifica e /o di controllo).

Colui il quale riceva la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di violazione di dati personali, deve darne immediata notizia al Dirigente / Responsabile di P.O. competente in relazione al trattamento dei dati personali, il quale conduce l'analisi volta ad individuare il grado di probabilità che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. Tale analisi è condotta congiuntamente ad altri Dirigenti / Responsabili di P.O. in caso di trattamento di dati personali coinvolgente diversi uffici o servizi e dev'essere accompagnata dall'acquisizione di ogni documento ed informazioni utile allo scopo.

Il Dirigente / Responsabile di P.O. competente in ragione del trattamento coinvolto, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede ad informare immediatamente il Sindaco ed il Responsabile della protezione dei dati personali, direttamente ovvero attraverso la figura del Referente, se istituita, nonché alla notifica della violazione all'Autorità di controllo.

La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Qualora la notifica effettuata nelle 72 ore non sia completa è possibile integrarla in una o più fasi successive (ad es. nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo).

Nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.

Il Responsabile del trattamento eventualmente coinvolto deve:
a) informare l'Ufficio tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Comune e sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza all'Ufficio per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive
azioni correttive all'Ufficio ed attuando tutte le azioni correttive approvate e/o richieste dall'Ufficio medesimo. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito.

Risulta opportuno e di particolare importanza che tutti gli atti di designazione a Responsabile del trattamento contengano una espressa previsione circa la necessità di informare il Comune, senza ingiustificato ritardo, in caso di avvenuta conoscenza di una violazione di dati personali, anche solo probabile o possibile.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
a) danni fisici, materiali o immateriali alle persone fisiche;
b) perdita del controllo dei dati personali;
c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale.
f) decifratura non autorizzata della pseudonimizzazione;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Ove il Dirigente / Responsabile di P.O. ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. Prima di procedere alla comunicazione della violazione ai soggetti interessati il testo della comunicazione, le modalità di notifica e le evidenze che attestano il reale livello di pregiudizio, dovranno essere concordate con il Responsabile della protezione dei dati personali. Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche sull'evento Data Breach, il Dirigente /

Responsabile di P.O. può chiedere all'Autorità di controllo l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

La probabilità e la gravità del rischio, per i diritti e le libertà dell'interessato, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica all'Autorità di controllo deve avere il contenuto minimo previsto dall'art. 33 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.

Ciascun Ufficio deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.

E' comunque opportuno che l'inventario delle violazioni tenga traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione. L'inventario dovrà essere dotato di idonee misure di sicurezza atte a garantire l'integrità e l'immodificabilità dei dati in esso registrati.

Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di controllo al fine di verificare il rispetto delle disposizioni del GDPR.

PARTE IV - DIRITTI DELL'INTERESSATO

INFORMATIVA, COMUNICAZIONE E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Il Comune adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR nonché per gestire le comunicazioni in merito all'esercizio dei diritti riconosciuti dal GDPR in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni di cui agli articoli 13 e 14 del GDPR sono fornite mediante predisposizione di idonea pagina web sul sito istituzionale e mediante pubblicazione del relativo testo all'Albo pretorio e nella sezione Amministrazione trasparente del portale (Informativa estesa). Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del Comune è predisposta apposita informativa.

Una informativa breve è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti ai quali l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture comunali, nelle sale d'attesa ed in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- in apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Comune;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutte le comunicazioni dirette all'Amministrazione;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, ecc..

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Il Comune agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18 del GDPR. Nei casi di cui all'articolo 11, paragrafo 2, del GDPR il Comune non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che dimostri che di non essere in grado di identificare l'interessato.

Il Comune fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta di esercizio dei diritti riconosciuti dal GDPR, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Comune informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Se non ottempera alla richiesta dell'interessato, il Comune informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese sulla base dei diritti riconosciuti dal GDPR sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Comune può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta. Incombe al Comune l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Fatto salvo l'articolo 11 del GDPR, qualora il Comune nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di esercizio dei diritti riconosciuti dal GDPR, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

ALLEGATI

1) Elenco delle principali Finalità del trattamento dei dati personali;
2) Modello di designazione di soggetto autorizzato al trattamento;
3) Modello di designazione di Dirigente / Responsabile di P.O.;
4) Modello di designazione del Segretario / Referente;
5) Designazione Amministratore di sistema;
6) Appendice contrattuale per il Responsabile del trattamento;
7) Nomina a Responsabile della protezione dei dati personali
8) Esempi di informative

ALLEGATO "1"
FINALITA DI TRATTAMENTO
(elencazione esemplificativa e non esaustiva)

principali finalità in relazione al trattamento dei dati personali dei cittadini

1. Servizi demografici / Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE), compresi l'acquisizione delle manifestazioni di consenso al trapianto di organi ed il rilascio di certificati e documenti di identità personale;
2. Servizi demografici / Stato civile - Attività di gestione dei registri di stato civile, attività in materia di cittadinanza, divorzi, separazioni e testamento biologico (DAT) nonché rilascio di certificati;
3. Servizi demografici / Cimiteri - Gestione cimiteri, concessioni, contributi, liquidazioni, retrocessioni, trasporti funebri ed attività correlate;
4. Servizi demografici / Leva - Attività relativa alla tenuta delle liste di leva, dei registri matricolari e dei registri dei congedi;
5. Servizi demografici / Leva - Attività relativa alla tenuta del registro degli obiettori di coscienza;
6. Servizi demografici / Elettorale - Attività relativa alla tenuta dell'elenco dei giudici popolari;
7. Servizi demografici / Elettorale - Attività relativa all'elettorato attivo e passivo con riferimento a consultazioni elettorali o referendarie comunitarie, nazionali o locali;
8. Servizi demografici / Elettorale - Attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio;
9. Servizi demografici / Statistica - Statistiche demografiche e rilevazioni richieste da ISTAT e altri enti;

10. Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria;
11. Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa;
12. Polizia municipale - Gestione delle procedure sanzionatorie, anche in fase contenziosa;
13. Polizia municipale - Attività relativa alla concessione di permessi di transito veicolate nelle zone a traffico limitato, controlli anche elettronici: varchi zone ZTL, rilevazioni rosso semaforico, coperture assicurative e tasse automobilistiche;
14. Polizia municipale - Attività relativa all'infortunistica stradale;
15. Polizia municipale – Attività delegata da Autorità pubblica e/o Organismi di controllo in materia di ordine e sicurezza pubblica ed amministrazione della giustizia;
16. Polizia municipale – Attività delegata di polizia giudiziaria;
17. Polizia municipale – Attività relative al rilascio di autorizzazioni (invalidi, circolazione in deroga a divieti, passi carrai, allaccio fognatura, occupazione suolo pubblico, ecc…);
18. Istruzione e cultura - Attività per la gestione di asili nido e scuole dell'infanzia e primaria (iscrizione, rinuncia, decadenza, rette, …);
19. Istruzione e cultura - Attività per la gestione dei servizi scolastici (mense, pasti, diete, intolleranze, motivi religiosi, pre e post scuola, trasporto studenti, centri estivi);
20. Istruzione e cultura - Attività di animazione (centri anziani, asili nido e scuole, gite, aree pubbliche e private, manifestazioni, ecc..) che comportano l'acquisizione di immagini fotografiche, filmati, registrazioni audio, ecc… (compresa la parte amministrativa ed organizzativa degli eventi);
21. Istruzione e cultura - Manifestazioni ed eventi, attività di ricreazione, cultura, sportive e di volontariato non ricomprese nella attività di animazione (inclusi: autorizzazioni, concessione di aree o locali, patrocini, organizzazione o supervisione, contributi e sovvenzioni);
22. Istruzione e cultura - Gestione delle biblioteche e dei centri di documentazione;
23. Istruzione e cultura - Attività di formazione ed informazione in favore del diritto allo studio (compresa la valorizzazione del tempo libero, il supporto all'istruzione ed assistenza scolastica);
24. Politiche del lavoro - Gestione delle attività relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale;
25. Commercio e agricoltura – regolamentazione delle attività di commercio in sede fissa, settore agricolo ed artigianale comprese autorizzazioni per manifestazioni fieristiche (in particolare, ed indicativamente, in materia di igiene e sicurezza sul lavoro; somministrazione di alimenti e bevande; servizi a tutela di consumatori ed utenti ed autorizzazioni; concessioni, permessi, licenze e nulla-osta (adozione dei provvedimenti di rilascio e attività connesse; individuazione degli aventi diritto, verifica e controllo delle condizioni), sussidi e sovvenzioni; gestione delle Sportello Unico attività produttive ed attività collaterali (SUAP);
26. Ambiente ed Animali - difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione compreso il rilascio di autorizzazioni, concessioni, permessi, licenze e nulla-osta (adozione dei provvedimenti di rilascio ed attività connesse; individuazione degli aventi diritto, verifica e controllo delle condizioni);
27. Ambiente ed Animali - Gestione delle attività di raccolta e smaltimento dei rifiuti (servizio, segnalazioni, accertamenti, sanzioni, ecc..);
28. Ambiente ed Animali - Gestione Anagrafe canina e benessere Animale (per anagrafe canina ambiti di sola conservazione/consultazione per passaggio competenza ad ASL dal 01/01/2006);
29. Edilizia ed urbanistica - pianificazione urbanistica, amministrazione del territorio, controlli su illeciti edilizi, autorizzazioni, concessioni, permessi, licenze e nulla-osta (adozione dei provvedimenti di rilascio ed attività connesse; individuazione degli aventi diritto, verifica e controllo delle condizioni);
30. Gestione del demanio e del patrimonio mobiliare ed immobiliare (lasciti e donazioni, alienazioni, vendite, locazioni, assegnazione o concessione, anche a titolo gratuito, a soggetti terzi di beni e spazi comunali per l'esecuzione di attività nel pubblico interesse, …) ivi incluso il profilo della protezione dei locali comunali, il controllo di particolari aree o strumenti ai fini di tutela di persone, beni e dati;
31. Espropri ed occupazioni - Attività volte all'acquisizione di proprietà o altri diritti reali su beni anche contro la volontà dei proprietari per esigenze di pubblico interesse;
32. Opere pubbliche - progettazione, manutenzione, affidamento o esecuzione di opere pubbliche, gestione tecnico amministrativa delle opere;
33. Entrate / Tributi - Gestione delle entrate tributarie dell'ente, ivi comprese le attività di accertamento e riscossione di tasse ed imposte;
34. Entrate / Tributi - Interventi di interesse pubblico a carattere sociale per particolari categorie di cittadini inerenti la riduzione delle imposte comunali o la riduzione di tariffe per l'accesso ai servizi educativi e sociali;
35. Messo comunale – attività relativa alla notificazione di atti e documenti;
36. Archivio e protocollo - Gestione della corrispondenza; tenuta del registro di protocollo; tenuta degli archivi e dei sistemi documentali dell'ente nonché l'archiviazione di atti e documenti nel pubblico interesse; conservazione sostitutiva; gestione del patrimonio culturale nazionale; conservazione, ordinamento e comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati

dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

37. Albo pretorio – gestione della pubblicazione legale mediante diffusione di atti e documenti anche a seguito istanza di terzi;

38. Attività di controllo delle autocertificazioni prodotte dagli interessati;

39. Sistema informativo - gestione del sistema informativo dell'ente (sistemi di salvataggio e ripristino, sicurezza, utenti e accessi alle risorse, progettazione, acquisizione, installazione e mantenimento, amministrazione di fornitori, contratti, ordini, consegne, fatture) compresa la gestione dei sistemi di posta elettronica (PEC e PEO), delle credenziali di identità digitale, dei sistemi di trasmissione dati e documentali, dei sistemi per la conservazione (locale e sostitutiva) di atti e documenti informatici; Supporto agli altri servizi dell'ente;

40. Sistema di videosorveglianza - esecuzione di compiti nell'interesse pubblico per la protezione e l'incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati, al controllo degli accessi in edifici pubblici; rilevazione infrazioni al codice della strada, accesso alle zone a traffico limitato, coperture assicurative e permessi invalidi; accertamento illeciti amministrativi in materia ambientale;

41. Promozione ed informazione - Servizi di promozione ed informazione in merito ad attività o eventi promossi o partecipati dall'Ente, alla viabilità, allarmi, avvisi, scadenze, emergenze, richieste di contatto, comunicazione di avvenuta notifica, ecc.. e, in generale, servizi vari di contatto resi anche tramite l'utilizzo dei recapiti telefonici e telematici, di internet o social network;

42. Servizi on-line - Servizi a cittadini, imprese, enti ed altri soggetti erogati attraverso il web o le reti sociali mediante processi di "e-government", compresa la diffusione di dati, atti e notizie; il rilascio di certificazioni; la prenotazione di appuntamenti; l'invio di questionari, newsletter; comunicazioni di dati, atti, documenti; connessioni WI-FI pubbliche, ecc...;

43. Protezione civile - Svolgimento di attività nel pubblico interesse ed in situazioni di emergenza (previsione e prevenzione dei rischi, soccorso alla popolazione colpite, contrasto e superamento dell'emergenza, e mitigazione del rischio);

44. Protezione civile - Attività mirate all'erogazione (anche ad opera di terzi) di contributi per eventi eccezionali (terremoti, alluvioni, frane ecc…);

45. Segnalazioni - Attività svolte nel pubblico interesse per la raccolta di segnalazioni sulla presenza sul territorio di situazioni per la quali viene ritenuto necessario l'intervento dell'ente (verde pubblico, dissesti stradali ecc…) e attività di raccolta di suggerimenti;

46. Gestione economica dell'Ente - adempimenti di obblighi fiscali o contabili, gestione dei fornitori (amministrazione di contratti, ordini, arrivi, fatture; selezioni in rapporto alle necessità), gestione contabile o di tesoreria (amministrazione della contabilità individuale e della contabilità risparmi), strumenti di pagamento elettronico (carte di credito e di debito; moneta elettronica), gestione della fatturazione elettronica attiva e passiva, erogazione di finanziamenti, sussidi e sovvenzioni (individuazione degli aventi diritto, calcolo, monitoraggio) ed attività di economato e provveditorato;

47. Contratti - Gestione dei contratti stipulati dall'ente, gestione dei fornitori (amministrazione dei fornitori; amministrazione di contratti, ordini, arrivi, fatture; selezioni in rapporto alle necessità), del contenzioso, dei procedimenti amministrativi per l'acquisizione di beni e servizi ed altre attività amministrative e contabili in materia; adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale; produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto; accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto;

48. Adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo;

49. Accordi e convenzioni - Attività interne di pubblico interesse inerenti la stipula di accordi, convenzioni e protocolli di intesa nelle varie materie di competenza dell'ente con altri soggetti pubblici o soggetti privati per disciplinare lo svolgimento di attività di interesse comune;

50. Servizi pubblici e Società partecipate - Attività per l'esternalizzazione anche parziale di servizi o funzioni istituzionali; attività di verifica dell'efficacia, l'efficienza, l'economicità e la qualità delle attività svolte dalle società partecipate dall'ente nonché a valutare i possibili effetti che la loro situazione economico finanziaria può determinare sugli equilibri finanziari del Comune;

51. Assicurazioni – gestione del rapporto assicurativo, comprese le azioni per il risarcimento danni; accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

52. Organi istituzionali - attività legate alla gestione ed al funzionamento degli organi istituzionali del Comune, alla garanzia e tutela dei cittadini ed agli atti degli organi comunali (compreso il Difensore civico comunale, se istituito); esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

53. Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali, ivi compreso l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;

54. Attività riguardante gli istituti di democrazia diretta e svolgimento di attività nel pubblico interesse con lo scopo di garantire la partecipazione dei cittadini nella proposizione, gestione e attuazione di piani e progetti del Comune;

55. Conferimento di onorificenze e ricompense, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

56. Rapporti con gli enti del terzo settore; rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

57. Trasparenza ed anticorruzione - attività in materia di trasparenza amministrativa e di contrasto della corruzione e della illegalità nell'ente; diffusione di dati sui beneficiari dei provvedimenti di concessione sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e vantaggi economici di qualunque genere a persone ed enti pubblici e privati;

58. Accesso agli atti e documenti amministrativi; accesso civico e accesso generalizzato; accesso ex art. 10 TUEL;

59. Privacy - Attività legate all'applicazione della normativa in materia di protezione dei dati personali in adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate;

60. Avvocatura - Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione;

principali finalità in relazione al trattamento dei dati personali in ambito socio-assistenziale

1. Gestione sportelli di informazione e di accoglienza di segretariato sociale;
2. Servizio sociale professionale;
3. Riconoscimento diritti sociali, politiche sociali e famiglia;
4. Assistenza socio-assistenziale in regime di domiciliarità (quali, a mero titolo esemplificativo e non esaustivo, servizi educativi per minori e per disabili, interventi di sollievo diurno, assistenza alla comunicazione per disabili sensoriali, servizio di assistenza domiciliare, contributi economici a sostegno della domiciliarità, assistenza economica, reddito di inclusione, telesoccorso, progetti di inserimento lavorativo, …);
5. Interventi, anche di carattere sanitario, in favore di soggetti bisognosi o non autosufficienti o incapaci;
6. Servizio semiresidenziale di accoglienza diurna, a tempo pieno o parziale, offerto al disabile e/o alla sua famiglia;
7. Inserimento disabili, minori, adulti, anziani autosufficienti e non in strutture residenziali, anche in regime di ricovero coatto;
8. Interventi di integrazione delle rette in strutture convenzionate;
9. Assistenza alle famiglie in caso di adozioni, anche internazionali;
10. Attività amministrative correlate all'applicazione della disciplina in materia di tutela sociale della maternità e di interruzione volontaria della gravidanza, per la gestione di consultori familiari;
11. Assistenza all'affidamento familiare di minori o assistenza ad attività di support family;
12. Iniziative rivolte a tutti i genitori sui temi dell'educazione dei figli;
13. Assistenza e supporto a gruppi di auto mutuo aiuto;
14. Collaborazione con l'Autorità Giudiziaria per l'assistenza e la tutela del minore in situazioni pregiudizievoli;
15. Assistenza e supporto a percorsi di mediazione familiare;
16. Assistenza e supporto a spazi di incontro protetto tra bambini e genitori;
17. Gestione dello sportello pubblico per immigrati;
18. Servizio di mediazione culturale per favorire l'integrazione sociale dei cittadini stranieri;
19. Assistenza e supporto al servizio civile volontario ed attività di volontariato in genere;
20. Attività finalizzate a prevenire il disagio e promuovere la cultura e la socializzazione dei giovani, in particolare nei contesti territoriali più svantaggiati;
21. Sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale;
22. Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto;
23. Gestione di attività ricreative e per la promozione del benessere della persona;
24. Iniziative di vigilanza e di sostegno con riferimento al soggiorno dei nomadi;
25. Prevenzione, cura e riabilitazione degli stati di tossicodipendenza. Attività di sostegno economico ed amministrative connesse;
26. Assistenza nei confronti di minori, anche in relazione a vicende giudiziarie; vigilanza per affidamenti temporanei e indagini psico-sociali relative a provvedimenti di adozione anche internazionale;
27. Assistenza sanitaria e punto di accesso ai servizi socio-sanitari (PASS);
28. Trattamenti sanitari obbligatori (T.S.O.) ed assistenza sanitaria obbligatoria (A.S.O.);
29. Gestione di attività inerenti asili nido comunali, scuola dell'Infanzia, scuola Primaria, scuola Secondaria di primo grado, scuola Secondaria di secondo grado e centri estivi;
30. Assistenza in procedure di applicazione di istituti di protezione giuridica quali curatele, tutele, amministrazioni di sostegno;
31. Attività di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche, ivi compresi gli assegni ai nuclei familiari numerosi, agevolazioni e bonus fiscali per l'uso dell'energia elettrica, gas ed acqua ed assegni di maternità;
32. Adempimento di obblighi contrattuali e precontrattuali;
33. Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
34. Verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia;
35. Gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale;
36. Garantire la collaborazione e funzioni di assistenza giuridico-amministrativa nei confronti degli organi dell'ente in ordine alla conformita' dell'azione amministrativa alle leggi, allo Statuto e ai regolamenti;
37. Elaborazione di statistiche interne;
38. Ogni altra attività amministrativa e di supporto necessaria a consentire il perseguimento delle finalità precedenti ovvero volta a verificare il possesso dei requisiti per l'accesso ai servizi od al beneficio di agevolazioni e provvidenze;
39. Illustrare le attività dell'Ente ed il loro funzionamento, favorire l'accesso ai servizi offerti dall'Ente, promuovendone la conoscenza, promuovere conoscenze allargate ed approfondite su temi di rilevante interesse pubblico e sociale, promuovere l'immagine dell'Ente;
40. Servizi on-line - Servizi attraverso il web o le reti sociali mediante processi di "e-government", compresa la diffusione di dati, atti e notizie; il rilascio di certificazioni; la prenotazione di appuntamenti; l'invio di questionari, newsletter; comunicazioni di dati, atti, documenti; connessioni WI-FI pubbliche, ecc...;
41. Sistema di videosorveglianza - esecuzione di compiti nell'interesse pubblico per la protezione e l'incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati, al controllo degli accessi in edifici pubblici;
42. Rapporti con gli enti del terzo settore; rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
43. Albo pretorio – gestione della pubblicazione legale mediante diffusione di atti e documenti anche a seguito istanza di terzi;
44. Attività di controllo delle autocertificazioni prodotte dagli interessati;
45. Trasparenza ed anticorruzione - attività in materia di trasparenza amministrativa e di contrasto della corruzione e della illegalità nell'ente; diffusione di dati sui beneficiari dei provvedimenti di concessione sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e vantaggi economici di qualunque genere a persone ed enti pubblici e privati;
46. Segnalazioni - Attività svolte nel pubblico interesse per la raccolta di segnalazioni sulla presenza sul territorio di situazioni per la quali viene ritenuto necessario l'intervento dell'ente e attività di raccolta di suggerimenti;
47. Accesso agli atti e documenti amministrativi; accesso civico e accesso generalizzato; accesso ex art. 10 del TUEL;
48. Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali, ivi compreso l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;

49. Assicurazioni – gestione del rapporto assicurativo, comprese le azioni per il risarcimento danni; accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
50. Privacy - Attività legate all'applicazione della normativa in materia di protezione dei dati personali in adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate;
51. Avvocatura - Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione;

principali finalità in relazione al trattamento dei dati personali in ambito di gestione del personale

1. Gestione delle esigenze preliminari alla instaurazione di un rapporto di lavoro;
2. Instaurazione e gestione dei rapporti di lavoro dipendente di qualunque tipo, anche a tempo parziale o temporaneo e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato, compreso l'esercizio dell'attività disciplinare;
3. Incontro domanda/offerta di lavoro, comprese le attività relative alla formazione professionale, iscrizione e partecipazione a corsi, sia in Italia che all'estero;
4. Valutazione del curriculum professionale, dei profili e delle competenze professionali e loro aggiornamento; definizione dei piani di sviluppo individuali e di carriera; valutazione delle prestazioni;
5. Gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale;
6. Liquidazione e pagamento di sovvenzioni, contributi, sussidi ed attribuzione di vantaggi economici;
7. Pianificazione economica, predisposizione dei budgets e loro gestione, ivi incluso il controllo delle spese di viaggio;
8. Adempimenti connessi all'eventuale iscrizione sindacale ed al connesso esercizio dei diritti e delle prerogative sindacali;
9. Riconoscimento di benefici connessi all'invalidità civile per il personale e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa;
10. Adempimento di obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare (a mero titolo esemplificativo, la normativa fiscale, previdenziale ed assistenziale, in materia di sicurezza sui luoghi di lavoro e la normativa in materia di protezione dei dati personali);
11. Adempimento di obblighi derivanti da contratti di assicurazione diretti alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale, nonché per garantire le pari opportunità;
12. Dare seguito a richieste da parte dell'autorità amministrativa o giudiziaria competente e, più in generale, di soggetti pubblici nel rispetto delle formalità di legge;
13. Organizzazione e controllo - Attività interne di coordinamento, programmazione, analisi, controllo, organizzazione, razionalizzazione ed integrazione delle risorse nonché rapporti con soggetti esterni e definizione indicatori e reporting;
14. Verifica e controllo degli accessi fisici, ivi incluso l'utilizzo di impianti di video sorveglianza, accessi informatici, abilitazione e disabilitazione di badge elettronici e password, regolamentazione dell'accesso agli archivi, di qualunque specie, ai computer, ai data-base ed alla rete, alle segreterie telefoniche; gestione delle linee telefoniche e della corrispondenza, anche informatica, verifiche dell'utilizzo delle risorse informatiche ai fini esclusivi della tutela della sicurezza dei dati, inclusi quelli personali; gestione dei sistemi di posta elettronica (PEC e PEO), delle credenziali di identità digitale, dei sistemi di trasmissione dati e documentali, dei sistemi per la conservazione (locale e sostitutiva) di atti e documenti informatici
15. Gestione dei servizi interni alla struttura del Titolare, quali, ad esempio: predisposizione e distribuzione di rubriche telefoniche o altri elenchi (eventualmente contenenti oltre ai dati identificativi anche una fotografia); prenotazione di viaggi e/o trasporto e/o alloggio; servizi di cassa valuta; prenotazione di sale riunioni e servizi di catering e ristoranti; distribuzione di buoni mensa "ticket restaurant"; concessione in uso di beni dell'Ente quali autovetture, carte di credito, PC fissi e portatili, telefoni cellulari; locazione di appartamenti, residence; invio di comunicazioni periodiche riservate ai dipendenti; gestione della reperibilità dei dipendenti;
16. Promozione ed informazione - Servizi di promozione ed informazione in merito ad attività o eventi promossi o partecipati dall'Ente, alla viabilità, allarmi, avvisi, scadenze, emergenze, richieste di contatto, comunicazione di avvenuta notifica, ecc.. e, in generale, servizi vari di contatto resi anche tramite l'utilizzo dei recapiti telefonici e telematici, di internet o social network;
17. Statistica interna ed esterna;
18. Archivio e protocollo - Gestione della corrispondenza; tenuta del registro di protocollo; tenuta degli archivi e dei sistemi documentali dell'ente nonché l'archiviazione di atti e documenti nel pubblico interesse; conservazione sostitutiva; gestione del patrimonio culturale nazionale; conservazione, ordinamento e comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
19. Albo pretorio – gestione della pubblicazione legale mediante diffusione di atti e documenti anche a seguito istanza di terzi;
20. Attività di controllo delle autocertificazioni prodotte dagli interessati;
21. Trasparenza ed anticorruzione - attività in materia di trasparenza amministrativa e di contrasto della corruzione e della illegalità nell'ente;
22. Accesso agli atti e documenti amministrativi; accesso civico e accesso generalizzato; accesso ex art. 10 TUEL;
23. Privacy - Attività legate all'applicazione della normativa in materia di protezione dei dati personali in adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate;
24. Avvocatura - Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione;

principali finalità in relazione al trattamento dei dati personali in ambito di gestione dei fornitori

1. finalità strettamente connesse e strumentali alla instaurazione, gestione, anche amministrativa, ed esecuzione dei rapporti pre-contrattuali e contrattuali ed agli adempimenti degli obblighi contabili, fiscali, di tutela giudiziale e di ogni altra natura, comunque inerenti a tali finalità;
2. Gestione economica dell'Ente - adempimenti di obblighi fiscali o contabili, gestione dei fornitori (amministrazione di contratti, ordini, arrivi, fatture; selezioni in rapporto alle necessità), gestione contabile o di tesoreria (amministrazione della contabilità individuale e della contabilità risparmi), strumenti di pagamento elettronico (carte di credito e di debito; moneta elettronica), gestione della fatturazione elettronica attiva e

passiva, erogazione di finanziamenti, sussidi e sovvenzioni (individuazione degli aventi diritto, calcolo, monitoraggio) ed attività di economato e provveditorato;

3. Contratti - Gestione dei contratti stipulati dall'ente, gestione dei fornitori (amministrazione dei fornitori; amministrazione di contratti, ordini, arrivi, fatture; selezioni in rapporto alle necessità), del contenzioso, dei procedimenti amministrativi per l'acquisizione di beni e servizi ed altre attività amministrative e contabili in materia; adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale; produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto; accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto;

4. Adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo;

5. Attività di controllo delle autocertificazioni prodotte dagli interessati;

6. Privacy - Attività legate all'applicazione della normativa in materia di protezione dei dati personali in adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate;

7. Avvocatura - Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione;

ALLEGATO "2"
ATTO DI DESIGNAZIONE / AUTORIZZAZIONE
DEI DIPENDENTI

ALLA C.A. DEI DIPENDENTI

In qualità di *"Designato Responsabile al Trattamento"* dei dati personali da parte del Titolare, conformemente a quanto stabilito dal Regolamento UE 679/2016 e dalla normativa italiana vigente D.Lgs. 196/2003 e ss.mm.ii., si incarica la S.V. **quale Autorizzato del trattamento dei dati personali** gestiti al fine di adempiere alle attività operative assegnate dal Titolare nell'ambito del rapporto lavorativo intercorrente tra la sua persona e lo stesso Titolare del trattamento dei dati.

Nell'ambito dello svolgimento del suo lavoro le raccomando l'adozione ed il monitoraggio delle seguenti misure di sicurezza, atte a impedire eventuali accessi abusivi ai dati personali detenuti sotto la responsabilità del Titolare del trattamento.

RACCOMANDAZIONI E ISTRUZIONI SULLA GESTIONE DEGLI ACCESSI NEL LUOGO DI LAVORO

È necessario ed opportuno da parte del personale autorizzato al trattamento dei dati personali:

- impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal *Titolare del Trattamento*;
- impedire il danneggiamento, la manomissione, la sottrazione, la distruzione, o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal *Titolare del Trattamento*;
- conservare i documenti contenenti i dati particolari/sensibili ai sensi del Regolamento UE 2016/679 in contenitori possibilmente muniti di serratura;
- verificare la corretta chiusura a chiave delle porte ogni qual volta lasciato incustodito l'ufficio;

BANCHE DATI TRATTATE (sia in formato cartaceo che elettronico):

SETTORE AMMINISTRATIVO

esempio- Segreteria generale e protocollo

GESTIONE DEI DISPOSITIVI ELETTRONICI, COMPUTER, TELEFONI AZIENDALI, PORTATILI.

SI RACCOMANDA fortemente di proteggere con password, da cambiare periodicamente per motivi di sicurezza, l'accesso a tutti i dispositivi elettronici in dotazione contenenti dati personali in modo da garantire:

- Protezione contro la perdita fisica dell'apparato;
- Protezione contro accesso non autorizzato ai dati;
- Trasferimento controllato e sicuro dei dati;
- Protezione contro la sottrazione o smarrimento;

In particolare, si raccomanda di attenersi a quanto disposto all'interno della "**Policy"** dell'ente riguardante l'utilizzo del materiale informatico, la stessa come anche il resto del materiale riguardante la privacy è disponibile all'interno di una cartella di rete condivisa denominata "Privacy", accessibile da parte di tutto il personale.

ULTERIORI RACCOMANDAZIONI DI SICUREZZA DIGITALE

- Si raccomanda sempre l'utilizzo dello strumento delle password, cambiandole ogni qual volta abbiate la sensazione che esse non ne siano sufficientemente sicure; laddove possibile, utilizzate sempre almeno 8 caratteri, mescolando caratteri maiuscoli, minuscoli e speciali;
- La parola chiave (password) deve essere preferibilmente priva di significato e non riconducibile in maniere elementare al soggetto che l'ha scelta e non deve mai essere comunicata a soggetti terzi, anche se fiduciari, a meno di diverse disposizioni del Titolare del trattamento;
- In caso di trattamento di dati particolari/sensibili la parola chiave (password) a protezione dei dispositivi elettronici deve sempre rispettare i criteri di scelta (8 caratteri alternando maiuscoli, minuscoli e speciali) ed essere aggiornata almeno ogni 6 mesi;
- Si raccomanda di evitare di utilizzare la stessa parola chiave (password) su più dispositivi elettronici;
- Si ricorda che la password di accesso ai dispositivi è segreta e strettamente personale, per tutto il perdurare del rapporto lavorativo;
- Si raccomanda fortemente di salvare tutto il lavoro svolto durante l'attività quotidiana, con particolare riferimento a quello contenente dati personali, sul server in modo da impedire la perdita dei dati stessi;

Si ricorda che tutti i designati al trattamento sono tenuti al rispetto della normativa vigente in materia di tutela dei dati personali, di cui al Regolamento (UE) 2016/679 e a conformare il trattamento dei dati secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

Si ricorda che le operazioni di trattamento dei dati personali devono essere eseguite esclusivamente per gli scopi inerenti l'attività svolta dalla Provincia e nel rispetto dei principi di cui all'art. 5 del citato Regolamento. In particolare, nel trattare i dati personali contenuti in documenti cartacei, i designati al trattamento sono tenuti, fra l'altro, a:

- custodire con la cura necessaria, al fine di garantirne la massima riservatezza, i documenti contenenti i dati personali in un armadio o in un cassetto chiusi a chiave o comunque non accessibili alle persone non autorizzate;
- raccogliere prontamente, nel caso di stampanti di rete o fax ubicati in locali comuni (ad es. corridoi), i documenti stampati o ricevuti via fax, soprattutto se contenenti dati personali, in modo da preservarne la riservatezza dei contenuti;
- conservare con le dovute cautele le chiavi utilizzate per i cassetti e gli armadi dove sono conservati i documenti contenenti dati personali;
- custodire con cautela le credenziali di autorizzazione per l'accesso ai locali ove previste (es. badge, chiavi, tessere identificative, ecc.);
- dare immediata comunicazione al responsabile dei sistemi informativi dell'Ente dell'eventuale smarrimento delle credenziali istituzionali;

ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 48 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Per **"Violazione di dati**" si intende 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 (Art. 4 p.12 del GDPR).

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?

Una 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;

- il furto o la perdita di dispositivi informatici contenenti dati personali;

- la deliberata alterazione di dati personali;

- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;

- la divulgazione non autorizzata dei dati personali.

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 48 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Il responsabile del trattamento e/o persona autorizzata o designata dal titolare che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare E IL DPO in modo che possano attivarsi.

DATA

PER PRESA VISIONE E ACCETTAZIONE DA PARTE DEL PERSONALE AUTORIZZATO

_____

FIRMA DESIGNATO DEL TRATTAMENTO

ALLEGATO "3"
ATTO DI DESIGNAZIONE / AUTORIZZAZIONE
DEI DIRIGENTI / RESPONSABILI P.O.

NOMINA E ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI AL PERSONALE DESIGNATO

Il Comune di Ottana, in qualità di *"Titolare del Trattamento"* dei dati personali, conformemente a quanto stabilito dal Regolamento UE 679/2016 e dalla normativa italiana vigente D.Lgs. 196/2003 e ss.mm.ii., si incarica la S.V. quale designato del trattamento dei dati personali gestiti al fine di adempiere alle attività operative assegnate dal Titolare nell'ambito del rapporto lavorativo intercorrente tra la sua persona e lo stesso Titolare del trattamento dei dati.

Nell'ambito dello svolgimento del suo lavoro le raccomando l'adozione ed il monitoraggio delle seguenti misure di sicurezza, atte a impedire eventuali accessi abusivi ai dati personali detenuti sotto la responsabilità del Titolare del trattamento.

NOMINA

I RESPONSABILI DI SETTORE quali **Designato Privacy** per il trattamento dei dati personali del proprio settore.

Occorre precisare che essi in qualità di Designato del settore, avranno i seguenti compiti:

- essere membro del Gruppo di Lavoro che supporta il Titolare, il DPO ed il Referente Generale per la Privacy per tutte le attività in materia di trattamento dei dati all'interno dell'ente;
- controllare il rispetto delle istruzioni in materia di trattamento di dati personali a carico dei propri collaboratori e all'interno del proprio settore;
- aggiornare, di concerto con il Dirigente di settore, il Registro dei trattamenti, di cui all'art. 30 del Reg. Ue n. 679/2016, relativamente al proprio settore di competenza;
- aggiornare le informative verso gli interessati;
- supportare le funzioni dell'Ente nelle nomine verso il personale autorizzato, Responsabili esterni del trattamento, altre funzioni;
- supportare l'Amministratore di sistema nell'applicazione del provvedimento a suo carico;
- supportare le funzioni dell'Ente nell'applicazione di specifici provvedimenti emessi dal Garante;
- supportare il DPO ed il Referente Generale per eventuali situazioni di Data Breach che si dovessero verificare all'interno del proprio settore;
- partecipare a riunioni ogni qualvolta si introduca all'interno dell'Ente una nuova tecnologia o debbano essere attuate campagne o operazioni che riguardino il trattamento dei dati personali e impostare unitamente al Titolare del trattamento la valutazione preventiva di impatto del rischio;
- partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche dell'ente che impattano sulla riservatezza dei dipendenti;

- conservare l'archivio della documentazione richiesta dal GDPR in riferimento al proprio settore;
- mettere in atto le disposizioni richieste dal DPO in materia di protezione dei dati;
- relazionare sullo stato di avanzamento ed eventuali problematiche;
- supportare il DPO nel predisporre e tenere sotto controllo il piano delle attività previste;
- supportare il DPO nel pianificare e condurre o sorvegliare la conduzione di attività di audit (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul GDPR);
- tenere sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso dell'audit;
- supportare il DPO nel tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi;

RACCOMANDAZIONI E ISTRUZIONI SULLA GESTIONE DEGLI ACCESSI NEL LUOGO DI LAVORO

È necessario ed opportuno da parte dei designati al trattamento dei dati personali:

- impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal *Titolare del Trattamento*;
- impedire il danneggiamento, la manomissione, la sottrazione, la distruzione, o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal *Titolare del Trattamento*;
- conservare i documenti contenenti i dati particolari/sensibili ai sensi del Regolamento UE 2016/679 in contenitori possibilmente muniti di serratura;
- verificare la corretta chiusura a chiave delle porte ogni qual volta lasciato incustodito l'ufficio;

GESTIONE DEI DISPOSITIVI ELETTRONICI, COMPUTER, TELEFONI AZIENDALI, PORTATILI.

SI RACCOMANDA fortemente di proteggere con password, da cambiare periodicamente per motivi di sicurezza, l'accesso a tutti i dispositivi elettronici in dotazione contenenti dati personali in modo da garantire:

- Protezione contro la perdita fisica dell'apparato;
- Protezione contro accesso non autorizzato ai dati;
- Trasferimento controllato e sicuro dei dati;
- Protezione contro la sottrazione o smarrimento;

In particolare, si raccomanda di attenersi a quanto disposto all'interno della "**Policy"** dell'ente riguardante l'utilizzo del materiale informatico, la stessa come anche il resto del materiale riguardante la privacy è disponibile all'interno di una cartella di rete condivisa denominata "Privacy", accessibile da parte di tutto il personale.

Si ricorda che le operazioni di trattamento dei dati personali devono essere eseguite esclusivamente per gli scopi inerenti l'attività svolta nel rispetto dei principi di cui all'art. 5 del citato Regolamento. In particolare, nel trattare i dati personali contenuti in documenti cartacei, i designati al trattamento sono tenuti, fra l'altro, a:

- custodire con la cura necessaria, al fine di garantirne la massima riservatezza, i documenti contenenti i dati personali in un armadio o in un cassetto chiusi a chiave o comunque non accessibili alle persone non autorizzate;
- raccogliere prontamente, nel caso di stampanti di rete o fax ubicati in locali comuni (ad es. corridoi), i documenti stampati o ricevuti via fax, soprattutto se contenenti dati personali, in modo da preservarne la riservatezza dei contenuti;
- conservare con le dovute cautele le chiavi utilizzate per i cassetti e gli armadi dove sono conservati i documenti contenenti dati personali;
- custodire con cautela le credenziali di autorizzazione per l'accesso ai locali ove previste (es. badge, chiavi, tessere identificative, ecc.);
- dare immediata comunicazione al responsabile dei sistemi informativi dell'Ente dell'eventuale smarrimento delle credenziali istituzionali;

ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 48 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Per **"Violazione di dati**" si intende 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 (Art. 4 p.12 del GDPR).

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?

Una 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;

- il furto o la perdita di dispositivi informatici contenenti dati personali;

- la deliberata alterazione di dati personali;

- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;

- la divulgazione non autorizzata dei dati personali.

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 48 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Il designato dal titolare che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare E IL DPO in modo che possano attivarsi.

DATA

Firma per accettazione della nomina come Designato

_____

ALLEGATO "4"
ATTO DI DESIGNAZIONE
DEL SEGRETARIO COMUNALE / REFERENTE PRIVACY DELL'ENTE

NOMINA E ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI AL PERSONALE REFERENTE

Il Comune di Ottana in qualità di Titolare del trattamento dei dati personali, con sede in Ottana

PREMESSO CHE

Ai sensi dell'articolo 38 del GDPR, infatti il Titolare ha l'obbligo di assicurarsi che "il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali"; il Titolare inoltre sostiene "il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".

Si ravvisa dunque la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati - di individuare uno o più dipendenti interni all'Ente cui assegnare il compito di "Referente" al fine di supportare l'attività del Responsabile della Protezione dei dati personali (RPD o DPO), nelle seguenti attività:

a) informazione e consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori best practice in materia di analisi e valutazione dei rischi.

b) sorveglianza dell'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei software e della relativa documentazione tecnica;

d) cooperare con l'Autorità di controllo e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva prevista dall'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.

Il Referente è tenuto al segreto od alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al RPD ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.

Tutto ciò premesso il titolare,

NOMINA

La dr.ssa Marilena Pirisi quale **Referente Privacy dell'ente** Comune di OTTANA per il trattamento dei dati personali

Occorre precisare che Ella, in qualità di Referente Privacy del settore, avrà i seguenti compiti:

- essere membro del Gruppo di Lavoro che supporta il Titolare, il DPO ed il Referente Generale per la Privacy per tutte le attività in materia di trattamento dei dati all'interno dell'ente;
- controllare il rispetto delle istruzioni in materia di trattamento di dati personali a carico dei propri collaboratori e all'interno del proprio settore;
- aggiornare, di concerto con il Dirigente di settore, il Registro dei trattamenti, di cui all'art. 30 del Reg. Ue n. 679/2016, relativamente al proprio settore di competenza;
- aggiornare le informative verso gli interessati;
- supportare le funzioni dell'Ente nelle nomine verso il personale autorizzato, Responsabili esterni del trattamento, altre funzioni;
- supportare l'Amministratore di sistema nell'applicazione del provvedimento a suo carico;
- supportare le funzioni dell'Ente nell'applicazione di specifici provvedimenti emessi dal Garante;
- supportare il DPO ed il Referente Generale per eventuali situazioni di Data Breach che si dovessero verificare all'interno del proprio settore;
- partecipare a riunioni ogni qualvolta si introduca all'interno dell'Ente una nuova tecnologia o debbano essere attuate campagne o operazioni che riguardino il trattamento dei dati personali e impostare unitamente al Titolare del trattamento la valutazione preventiva di impatto del rischio;
- partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche dell'ente che impattano sulla riservatezza dei dipendenti;
- conservare l'archivio della documentazione richiesta dal GDPR in riferimento al proprio settore;
- mettere in atto le disposizioni richieste dal DPO in materia di protezione dei dati;
- relazionare sullo stato di avanzamento ed eventuali problematiche;
- supportare il DPO nel predisporre e tenere sotto controllo il piano delle attività previste;
- supportare il DPO nel pianificare e condurre o sorvegliare la conduzione di attività di audit (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul GDPR);
- tenere sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso dell'audit;
- supportare il DPO nel tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi;

DATA

Firma per accettazione della nomina come Referente privacy

_____

ALLEGATO "5"
AMMINISTRATORE DI SISTEMA

OGGETTO: NOMINA E ISTRUZIONI AMMINISTRATORE DI SISTEMA

In conformità alla normativa vigente ed in particolare al provvedimento del Garante della Privacy del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), così come modificato con Provvedimento del 25/6/2009, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici" relativamente alle attribuzioni delle funzioni di Amministratore di Sistema, il Dirigente del Servizio Risorse e Sistema Informativo, valutate le qualità tecniche, professionali e di condotta

nomina

il Sig. [_____] nato a [_____] il [_____] per suo conto/in qualità di [_____] della società [_____] con sede in [_____] Via[_____] n.[___]

Amministratore di Sistema

Nello specifico gli ambiti operativi di competenza della S.V. sono i seguenti *(specificare l'ambito di operatività per settori o per aree applicative)*:

- .....
- .....
- .....
- .....

In particolare, sarà specifico compito della S.V., nell'ambito della protezione dei dati personali ai sensi del suddetto provvedimento del Garante e della normativa sulla protezione dei dati personali:

1. attribuire a ciascun designato/autorizzato al trattamento un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice non potrà, neppure in tempi diversi, essere assegnato a persone diverse;
2. assegnare e gestire i codici identificativi personali prevedendone la disattivazione nel caso di perdita della qualità che ne consente l'accesso all'elaboratore, ovvero nel caso di loro mancato utilizzo per un periodo superiore a sei mesi;
3. disporre ogni opportuna misura e ogni adeguata verifica, per evitare che soggetti non autorizzati possano avere accesso agli archivi delle parole chiave se leggibili;
4. predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ovvero ai sistemi di trasmissione dati o di sicurezza e agli archivi elettronici che vengono effettuati dagli Amministratori di Sistema, assicurando che tali registrazioni (access log) abbiano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
5. predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;

6. provvedere affinché gli elaboratori del sistema informativo siano protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615 *quinquies* cod.pen., mediante idonei programmi la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale;
7. assistere il Responsabile del trattamento / Responsabile della Protezione dei dati personali in particolare per quanto concerne l'analisi dei rischi presso la propria Struttura e per le informazioni che il Responsabile è tenuto ad inviare periodicamente al Titolare per l'aggiornamento della valutazione delle misure di sicurezza informatica dell'ente (utilizzando l'apposita check list dell'AGID);
8. Le ricordiamo che in base al provvedimento già citato l'Ente provvederà alla verifica almeno annuale delle attività svolte dagli Amministratori di Sistema in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

   La informiamo che gli estremi identificativi della S.V. saranno utilizzati secondo quanto stabilito dall'art. 4.3 del citato provvedimento.

   Tale nomina è a tempo indeterminato e decade per revoca, per dimissioni o con il venir meno delle mansioni svolte dalla S.V. che giustificano tale nomina. In caso di decadenza della nomina, il Responsabile del trattamento si impegna a comunicare tempestivamente al Titolare il nominativo del soggetto da nominare.

Data [_____]
Firma Dirigente del Servizio Risorse e Sistema Informativo[_____]

Per accettazione

L'Amministratore di Sistema
[_____]

ALLEGATO "6"
RESPONSABILE DEL TRATTAMENTO - APPENDICE CONTRATTUALE

NOMINA DI RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI

Il Comune di …… con sede in ……. - .., (di seguito, "il **Titolare**"), in relazione al Contratto (CIG _____) stipulato in data _____, concernente la fornitura/incarico di …… con la presente, ai sensi dell'art. 28 Reg. UE 2016/679 (di seguito "**RGPD**"),

NOMINA

…….. con sede legale a …….P:IVA……, rappresentata da …….., domiciliato presso la sede della società medesima, che stipula il presente atto in nome e per conto della società …….
RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

(di seguito il "**Responsabile**")

con riferimento a tutti i trattamenti effettuati nell'ambito dei rapporti contrattuali instaurati con il Titolare in virtù dei Contratti, nonché a quelli che in futuro dovessero rendersi necessari a seguito di modifiche e integrazioni dei predetti accordi.

Le incombenze e le responsabilità oggetto della Nomina vengono affidate al Responsabile sulla base delle dichiarazioni dallo stesso fornite all'Amministrazione circa le caratteristiche di esperienza, capacità e affidabilità che vengono richieste dalla normativa vigente (art. 28 Regolamento UE 2016/679) per chi esercita la funzione di Responsabile.

Con la sottoscrizione della presente lettera, il Responsabile si dichiara disponibile e competente per la piena attuazione di quanto ivi disposto, accetta la nomina, conferma la diretta ed approfondita conoscenza degli obblighi che assume in relazione al dettato del RGPD, conferma, altresì, di disporre di una propria organizzazione che dichiara idonea a consentire il trattamento dei dati nel pieno rispetto delle prescrizioni legislative, ivi compreso il profilo della sicurezza, e si impegna a procedere al trattamento dei dati personali attenendosi alle istruzioni impartite, nel pieno rispetto di quanto imposto dall'art. 28 del RGPD.

Onde consentire al Responsabile di espletare i compiti e le attribuzioni meglio specificati in seguito, con la presente Nomina vengono fornite le specifiche istruzioni per l'assolvimento del compito assegnato.

Resta inteso che la normativa applicabile comprende l'insieme delle norme rilevanti in materia di privacy e cioè il Regolamento europeo 2016/679 in materia di protezione dei dati personali (**RGPD**) e inoltre, in ogni tempo, ogni linea guida, norma di legge, codice o provvedimento rilasciato o emesso dagli organi competenti o da altre autorità di controllo.

1. ISTRUZIONI GENERALI AL RESPONSABILE

Il Responsabile - così individuato e nominato, in relazione ai trattamenti di dati personali rientranti nell'ambito operativo e funzionale di propria competenza - sebbene non in via esaustiva, avrà i compiti e le attribuzioni di seguito elencate e dunque dovrà:

1. trattare i dati personali secondo le istruzioni ricevute dal Titolare del trattamento;

2. effettuare la ricognizione delle banche dati e degli archivi elettronici relativi ai trattamenti effettuati in esecuzione delle Attività;

3. tenere un registro, come previsto dall'art. 30 del GDPR di tutte le categorie di attività relative al trattamento svolte per conto dell'Amministrazione in qualità di responsabile;

4. organizzare le strutture, gli uffici e le competenze necessarie e idonee a garantire il corretto espletamento delle Attività;

5. astenersi dal trattare i dati personali oggetto delle Attività per finalità proprie;

6. non diffondere o comunicare a terzi i dati trattati attraverso le Attività, al di fuori di quanto necessario per l'assolvimento di obblighi di legge o di contratto;

7. garantire l'affidabilità di qualsiasi dipendente che accede ai dati personali del Titolare ed assicurare, inoltre, che gli stessi abbiano ricevuto adeguate istruzioni e formazione (quali incaricati/autorizzati del trattamento) con riferimento alla protezione e gestione dei dati personali e che siano vincolati al rispetto di obblighi di riservatezza conformi alla presente Nomina. Il Responsabile esterno risponderà di eventuali violazioni ai sensi dell'art. 2049 del codice civile;

8. procedere alla nomina del proprio/i amministratore/i di sistema, in adempimento di quanto previsto dal provvedimento del Garante per la protezione dei dati personali (Garante Privacy) del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti, comunicandolo prontamente al Titolare, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;

9. assistere tempestivamente il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di procedere ad un DPIA (Valutazione di impatto sulla protezione dei dati) ai sensi art. 35 e ss. del RGPD, con obbligo di notifica quando venga a conoscenza di un trattamento di dati che possa comportare un rischio elevato;

10. assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32-36 RGPD, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile;

11. astenersi dal trasferire i dati personali trattati per conto dell'Amministrazione al di fuori dello Spazio Economico Europeo senza il previo consenso scritto della stessa; in caso di consenso, il Responsabile dovrà assicurarsi che il trattamento avvenga verso Paesi terzi e Organizzazioni internazionali che garantiscano un livello di sicurezza e protezione adeguato;

12. notificare all'Amministrazione, senza ingiustificato ritardo e comunque non oltre le ventiquattro (24) ore da quando ne abbia avuto conoscenza, ai sensi dell'art.33 del GDPR, se si sia verificato un *Data breach* anche presso i propri Sub-responsabili, adottando, di concerto con il Titolare, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente;

13. avvertire prontamente l'Amministrazione, entro tre (3) giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile inviando copia delle istanze ricevute all'indirizzo e-mail/PEC ……e assistere il Titolare del trattamento con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;

14. avvisare immediatamente, e comunque entro tre (3) giorni lavorativi, il Titolare del trattamento, di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria eventualmente ricevuta inviando copia delle istanze all'indirizzo PEC …….. per concordare congiuntamente il riscontro;

15. adottare adeguati processi e ogni altra misura tecnica idonea ad attuare le istruzioni fornite dal Titolare e predisporre idonee procedure interne finalizzate alla verifica periodica della corretta applicazione e della congruità degli adempimenti posti in essere.

Il Titolare si riserva, altresì, ove ne ravvisasse la necessità, di integrare e adeguare di volta in volta le presenti istruzioni.

2. MISURE TECNICHE ED ORGANIZZATIVE -AUDIT E DIRITTI DI VERIFICA DEL TITOLARE DEL TRATTAMENTO

Il Responsabile, oltre a quanto previsto dall'Allegato 1, si obbliga ad adottare ed implementare le misure tecniche ed organizzative di sicurezza (di seguito "**Misure"**) che – ai sensi dell'art. 32 RGPD siano adeguate ad eliminare o comunque a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, con l'obbligo di documentarle se richiesto dal Titolare.

Il Titolare si riserva la facoltà di effettuare, nei modi ritenuti più opportuni, anche tramite l'invio di propri funzionari a ciò delegati presso i locali del Responsabile o tramite l'invio di apposite *check list*, verifiche tese a vigilare sulla puntuale osservanza delle disposizioni di legge e delle presenti istruzioni.

In alternativa a quanto sopra precisato, il Responsabile può fornire al Titolare copie delle relative certificazioni esterne audit report e/o altra documentazione sufficiente per il Titolare a verificare la conformità del Responsabile alle Misure della presente Nomina.

3. CORREZIONI, CANCELLAZIONE O BLOCCO DI DATI

Il Responsabile può correggere, cancellare o bloccare il trattamento dei dati personali a beneficio del Titolare solo quando ha avuto istruzioni dal Titolare in tal senso. Se l'interessato fa richiesta direttamente al Responsabile per la correzione o la cancellazione dei propri dati personali, il Responsabile deve indirizzare la predetta richiesta al Titolare senza ritardo alcuno.

Alla scadenza della Nomina, il Responsabile si obbliga a restituire al Titolare tutti i dati in suo possesso, provvedendo ad eliminare definitivamente dal proprio sistema informativo e dagli archivi cartacei, i medesimi dati o copie degli stessi, dandone conferma per iscritto al Titolare.

4. SUB-RESPONSABILI

Per l'esecuzione delle Attività, il Responsabile può avvalersi di Sub-responsabili.

a. Designazione Sub-responsabili. Se il Responsabile ritiene opportuno o necessario nominare Sub-responsabili è autorizzato sin d'ora a nominarli, con l'obbligo di inoltrare la relativa documentazione al Titolare.

b. Obblighi verso il Sub-responsabile. Il Responsabile:

(i) limiterà l'accesso del Sub-responsabile ai dati personali a quanto strettamente necessario per soddisfare gli obblighi del Responsabile ai sensi della Nomina; al Sub-responsabile sarà vietato l'accesso ai dati personali per qualsiasi altro scopo;

(ii) imporrà per iscritto ad ogni Sub-responsabile il rispetto di obbligazioni ed istruzioni equipollenti a quelle previste nella presente Nomina nella sua totalità, ivi incluso l'Allegato 1, nonché la possibilità di effettuare audit;

(iii) rimarrà pienamente responsabile nei confronti del Titolare per il rispetto degli obblighi derivanti dalla presente Nomina per qualsiasi atto o omissione del Sub-responsabile che comporti una violazione degli stessi.

5. MANLEVA

Il Responsabile tiene indenne e manlevato il Titolare (e ciascuno dei suoi rispettivi dipendenti e agenti) da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura (sia essa prevedibile, contingente o meno) derivante da o in connessione con una qualsiasi violazione da parte del Responsabile degli obblighi della normativa applicabile o delle disposizioni contenute nella presente Nomina.

L'implementazione da parte del Responsabile delle misure tecniche e organizzative previste dal presente atto sarà effettuata nell'ambito delle attività contrattualmente pattuite e del relativo corrispettivo.

6. DURATA

La Nomina decorre dalla data della sua sottoscrizione e rimarrà in vigore sino alla risoluzione o scadenza dei Contratti o cessazione dei servizi da eseguirsi in relazione delle Attività.

7. MODIFICHE DELLE LEGGI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

Nell'eventualità di qualsivoglia modifica delle norme in materia di trattamento dei dati personali applicabili al trattamento dei dati personali effettuato dall'Amministrazione, che generi nuovi requisiti, il Responsabile del trattamento collaborerà, nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti durante l'esecuzione del contratto.

8. CONTATTI E REFERENTI

Le parti stabiliscono che i referenti per l'esecuzione della Nomina sono:

Per il Titolare del Trattamento: _____

Per il Responsabile del Trattamento: _____, (e-mail - tel)

Qualsiasi modifica relativa le sopra menzionate persone o la responsabilità delle persone di contatto deve essere immediatamente notificata all'altra parte.

Si allega, a costituire parte integrante e sostanziale della presente Nomina, l'all. 1 "Misure tecniche e organizzative di sicurezza"

Il Titolare del Trattamento **Il Responsabile, per conferma e accettazione**

_____ _____

ALLEGATO "7"
DECRETO DESIGNAZIONE DPO – RESPONSABILE PROTEZIONE DEI DATI

Oggetto:

Designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679

Premesso che

- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (di seguito RGPD), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, introduce la figura del Responsabile dei dati personali (RDP) (artt. 37-39);
- Il predetto Regolamento prevede l'obbligo per il titolare o il responsabile del trattamento di designare il RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali» (art. 37, paragrafo 1, lett a);
- Le predette disposizioni prevedono che il RPD «può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi» (art. 37, paragrafo 6) e deve essere individuato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39» (art. 37, paragrafo 5) e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento» (considerando n. 97 del RGPD);
- Le disposizioni prevedono inoltre che «un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o

organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione» (art. 37, paragrafo 3);

Confermato che

Il comune di ……

- è tenuto alla designazione obbligatoria del RPD nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD;
- con deliberazione del Consiglio Comunale n. … del …… è stato deliberato il trasferimento all'Unione dei Comuni ……– …….. il servizio di Responsabile per la Protezione Dati
- all'esito di procedura negoziata da parte dell'Unione dei Comuni Monte Linas – Dune di Piscinas finalizzata all'affidamento del "Servizio di Responsabile per la Protezione Dati (RPD) e supporto in materia di protezione dati personali", ha ritenuto che la Fondazione Logos PA, C.F. 02404510808, con sede legale in Via Lia 13 89100 (Reggio Calabria) nella persona dell'Avv. Mastrofini Roberto, sia in possesso del livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del RGPD, per la nomina a RPD, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare;

Visto

- Il D.lgs. 267/2000

DECRETA

Per quanto in premessa

Di designare

, Responsabile della Protezione dei Dati Personali (RPD) per il comune di OTTANA;

Di stabilire che

Il RPD, nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
- cooperare con il Garante per la protezione dei dati personali;
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

I compiti del Responsabile della Protezione dei Dati personali attengono all'insieme dei trattamenti di dati effettuati dal comune di OTTANA.

Di impegnare

Il comune di Ottana a:

- mettere a disposizione del RPD risorse necessarie al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni;
- non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
- garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse

i quali vengono allegati al presente atto del quale fanno parte integrante e sostanziale.

Di stabilire che

il nominativo e i dati di contatto del RPD (recapito postale, telefono, email) siano resi disponibili agli uffici dell'Ente. I dati di contatto saranno, altresì, pubblicati sul sito internet istituzionale

https://www.comune.ottana.nu.it/index.php

Di comunicare

Il nominativo e i dati di contatto del RPD al Garante per la protezione dei dati personali

Di pubblicare

il presente Decreto all'Albo Pretorio on line per 15 giorni consecutivi e, in modo permanente, sul sito istituzionale del Comune alla sezione Amministrazione Trasparente