COMUNE DI LEVONE

Provincia di Torino

PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO A TUTELA DEI DATI PERSONALI

Sommario

PREMESSA 3

PARTE I - NORME E PRINCIPI GENERALI 5

SENSIBILIZZAZIONE E FORMAZIONE 6

TRATTAMENTO DEI DATI PERSONALI 7

CIRCOLAZIONE DEI DATI PERSONALI 8

COORDINAMENTO DI NORME 8

PARTE II - PROFILO ORGANIZZATIVO 9

ORGANIGRAMMA PRIVACY 9

IL TITOLARE DEL TRATTAMENTO 10

L'AUTORIZZATO AL TRATTAMENTO 12

IL REFERENTE DEL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI 13

AMMINISTRATORE DEL SISTEMA INFORMATICO 14

IL RESPONSABILE ESTERNO DEL TRATTAMENTO 15

IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI 16

PARTE III - ADEMPIMENTI E PROCEDURE 17

MISURE PER LA SICUREZZA DEI DATI PERSONALI 17

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO 17

VALUTAZIONI DI IMPATTO SULLA PROTEZIONE DEI DATI 19

VIOLAZIONE DEI DATI PERSONALI 24

STIMA DI UNA VIOLAZIONE DI SICUREZZA CON RIFERIMENTO AI DIRITTI E ALLE LIBERTÀ DEGLI INTERESSATI 26

FLUSSO DEGLI ADEMPIMENTI IN CASO DI VIOLAZIONE DEI DATI.... **Errore. Il segnalibro non è definito.**

PARTE IV - DIRITTI DELL'INTERESSATO 28

INFORMATIVA, COMUNICAZIONE E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO 28

ALLEGATO: FINALITÀ DI TRATTAMENTO 29

GLOSSARIO

Accountability = letteralmente “rendere conto”, ovvero, il Titolare del trattamento si deve responsabilizzare autonomamente nella gestione ed organizzazione della Privacy. In questo modo, il Titolare di un trattamento dati non è più mero esecutore di un elenco di misure imposte ad una norma, ma diviene responsabile delle misure operative e tecniche che riterrà opportune, efficaci e dunque adeguate al fine di salvaguardare i dati che tratta. L’obiettivo di ogni titolare, responsabile e addetto al trattamento dei dati, sarà quello di essere accountable con il regolamento. Questo significa sostanzialmente non solo divenire responsabile delle scelte di mezzi, operazioni, procedure, finalità, etc. in materia di trattamento dei dati, ma anche essere in grado di “dare conto” delle valutazioni svolte alla base delle scelte poi operate.

Audit Privacy = è una valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Reg. UE n. 679/2016;

Data breach = è 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.

DPIA = Valutazione di impatto sulla protezione dei dati;

GEPD = Garante Europeo della protezione dei dati;

Privacy by design = Privacy dal momento della sua progettazione. Implica che qualsiasi progetto debba realizzato assumendo dalla fase iniziale di ideazione misure di protezione di dati personali;

Privacy by default = protezione dei dati per impostazione predefinita, ovvero, misure tecniche ed organizzative che assicurano solo i dati personali necessari per ogni specifica finalità di trattamento;

RGDP = Regolamento Generale sulla Protezione dei Dati Personali, Regolamento UE n. 679/2016;

RPD = Responsabile della Protezione dei dati (in inglese DPO, ovvero Data Protection Officer);

WP 29 = Warking Party Art. 29 (c.d. Gruppo di lavoro art. 29), ovvero organismo consultivo ed indipendente composto da un rappresentante dei Garanti dei dati personali di ogni stato membro, da un rappresentante della Commissione UE e dal Garante europeo della protezione dei dati.

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, in precedenza, 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 al fine di 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.

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, paragrafo 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 da anni, 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, l'ente 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 l'ente.
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 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 l'ente 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 all'articolo 30 del GDPR.

Tipologie di dati

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali l'ente tratta le seguenti tipologie di dati:

- dati personali, quali definiti all'articolo 4, paragrafo 1 del GDPR (ovvero *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*);
- categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR (ovvero *"dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"*) unicamente nei casi previsti dal paragrafo 2 del Regolamento stesso.

Finalità del trattamento

Il Comune effettua periodicamente una ricognizione delle finalità che impongono o consentono il trattamento dei dati personali, anche particolari.
Nel presente documento viene predisposto apposito elenco (a carattere esemplificativo e non esaustivo) delle principali finalità del trattamento (Allegato).

CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizioni normative che lo vietino, l'ente 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.

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

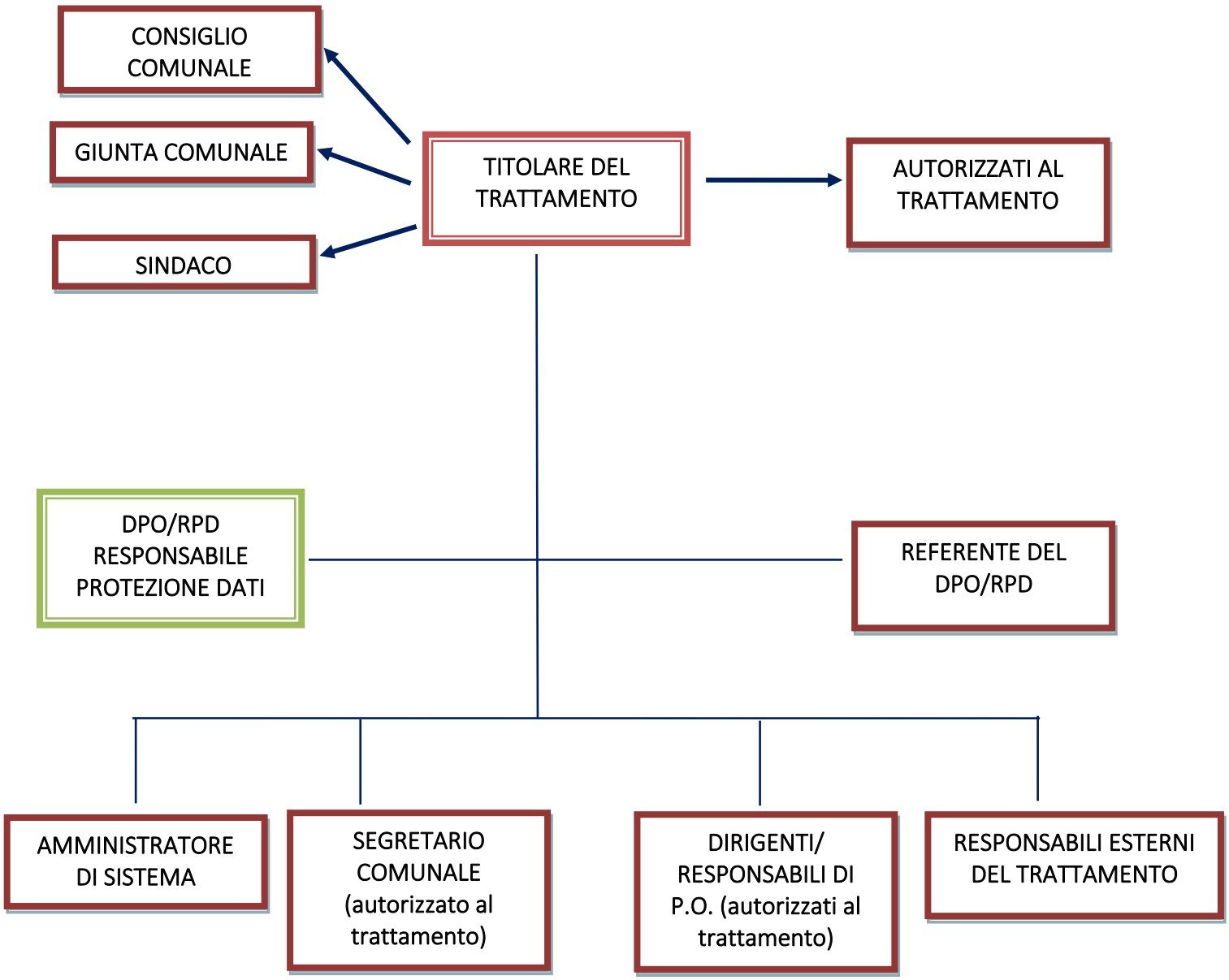
Profilo strutturale

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.

ORGANIGRAMMA PRIVACY



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 al fine di 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) e all'interessato (art. 34) eventuali violazioni dei dati;
j) ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
k) rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
l) 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;
j) 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;
k) redigere 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;
l) 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;
m) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;
n) individuare i responsabili (esterni) fornendo le necessarie indicazioni.

L'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 personale operante (a qualunque titolo ed a qualunque livello) all'interno dell'ente è conseguentemente autorizzato al compimento delle operazioni di trattamento dei dati necessari 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 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».

IL REFERENTE DEL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'articolo 38 del GDPR, 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 agli 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;

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;

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.

AMMINISTRATORE DEL SISTEMA INFORMATICO

Al fine di ottemperare a quanto disposto dal Garante della privacy alla luce del Regolamento UE 679/2016 attualmente in vigore, la nomina di un amministratore di sistema è un elemento fondamentale di accountability ai sensi dell'art. 24 del GDPR e di sicurezza ai sensi art. 32 dello stesso ove *"le cautele in materia di nomina di un amministratore di sistema non sono altro che alcune delle misure tecniche ed organizzative finalizzate a garantire la sicurezza dei trattamenti"* e altresì la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di trattamento dei dati personali.

Pertanto, sulla base anche di quanto sancito in precedenza 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 all'ente 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.

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 ESTERNO 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.

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 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.

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.
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 13 e 14 del GDPR.

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.
É intenzione dell'ente 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 (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.

Per un puntuale completamento del Registro dei trattamenti, occorrerà:

- 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.

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 Titolare del trattamento, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, 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 Titolare del trattamento 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 battuta, 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 Titolare del trattamento ritenga motivatamente che non possa presentare un rischio elevato; in relazione al trattamento interessato, il Titolare può comunque 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:

1. 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);
2. 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);
3. 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;
4. 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:
    - delle finalità specifiche, esplicite e legittime;
    - della liceità del trattamento;
    - dei dati adeguati, pertinenti e limitati a quanto necessario;
    - del periodo limitato di conservazione;
    - delle informazioni fornite agli interessati;
    - del diritto di accesso e portabilità dei dati;
    - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
    - dei rapporti con i responsabili del trattamento;
    - delle garanzie per i trasferimenti internazionali di dati;
    - 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.

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
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.
É 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.

La CNIL, l'Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai Titolari in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA).
Il software – gratuito, in continua evoluzione e liberamente scaricabile dal sito
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil - offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA (per le istruzioni si veda l'ultimo paragrafo del presente punto).
È bene, tuttavia, precisare che il software di cui sopra non costituisce un modello al quale fare riferimento in ogni situazione di trattamento, essendo stato concepito soprattutto come ausilio metodologico per le PMI. Offre in ogni caso un focus sugli elementi principali di cui si compone la procedura di valutazione d'impatto sulla protezione dei dati. Potrebbe costituire quindi un utile supporto 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.

<u>Istruzioni per l'installazione del software</u>

Una volta aperta la pagina https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil scorrere fino al titolo "Version logicielle" e selezionare il tipo di sistema operativo installato sul proprio computer.
Una volta scaricato il software, lanciare l'installazione che sarà effettuata automaticamente nella versione in lingua italiana.

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.). Pertanto, una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi di data breach sono:
- 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.

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).

Cosa fare in caso di violazione dei dati personali

Il titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 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 che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il Titolare in modo che possa attivarsi.
Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.
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 ("Registro delle violazioni"). Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Che tipo di violazioni di dati personali devono essere notificate?

Devono essere notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.
Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

Che informazioni deve contenere la notifica al Garante?

La notifica deve contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951).
Qualora si utilizzi per la notifica il modello allegato al provvedimento, è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

Come inviare la notifica al Garante?

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it oppure tramite posta elettronica ordinaria all'indirizzo protocollo@gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.
L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.

Per semplificare gli adempimenti previsti per i Titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) indicato sul sito https://servizi.gpdp.it/databreach/s/ che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Le azioni del Garante

Il Garante può prescrivere misure correttive (Articolo 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di euro.

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.
È, 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.

STIMA DI UNA VIOLAZIONE DI SICUREZZA CON RIFERIMENTO AI DIRITTI E ALLE LIBERTÀ DEGLI INTERESSATI

L'art. 33 del GDPR precisa che la notifica all'autorità di controllo deve essere svolta, secondo i tempi previsti, *"a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche"*.
Analogamente, ai sensi dell'art. 34, la comunicazione all'interessato è obbligatoria *"quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*, e nello specifico, non è richiesta se sono state messe in atto misure tecniche e organizzative adeguate di protezione ovvero se i dati personali sono stati resi incomprensibili (ad es. tramite cifratura), oppure se è stato prontamente scongiurato il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.
Sulla base di quanto riportato dal Regolamento, risulta evidente come una corretta gestione delle violazioni di dati personali debba inevitabilmente:

- tenere conto degli elementi tecnici e organizzativi che permettono di descrivere le circostanze della violazione stessa; quindi, anche sulla base di questi elementi;
- svolgere una valutazione sui rischi che guidi la decisione di notificare/comunicare la violazione.

L'ente ritiene che l'identificazione di un "criterio" o un metodo oggettivo e predefinito di valutazione sia una scelta in linea con il GDPR.
Il GDPR non specifica i metodi ritenuti adatti a valutare la presenza e l'entità dei rischi sui diritti e le libertà delle persone fisiche (lasciando pertanto una generale autonomia a ciascun Titolare del trattamento e il potere di scelta sulla modalità di approccio).

Per il principio di *accountability (responsabilizzazione)*, l'ente intende formalizzare un metodo e dei criteri da utilizzare per la valutazione, facendo riferimento alle indicazioni dell'ENISA (European Union Agency for Network and Information Security), l'Agenzia europea per la sicurezza delle reti e dell'informazione.
Il presente metodo è da intendersi solamente come strumento di supporto alla valutazione per il soggetto preposto alla stima della violazione, che potrà autonomamente scegliere di adottare una diversa modalità di giudizio.
Secondo il modello dell'ENISA, gli elementi centrali che devono essere presi in considerazione quando si valuta la gravità di una violazione di dati personali, sono:

- contesto del trattamento e tipologia di dati;
- facilità di identificazione dell'individuo sulla base dei dati violati;
- circostanze della violazione.

Al fine di definire un punteggio al parametro relativo al contesto del trattamento, l'ENISA suggerisce di attribuire un punteggio di base utilizzando come criterio la classe di dati violati, regolando poi il punteggio sulla base dell'analisi di altri fattori di contesto.
Per quanto concerne la facilità di identificazione, la valutazione di questo parametro avviene in relazione a quattro livelli di identificabilità crescente, il cui valore sarà utilizzato come moltiplicatore sul punteggio di base del contesto del trattamento.
Infine, gli elementi relativi alle circostanze della violazione sono rappresentati dalle perdite di riservatezza (la cui entità varierà a seconda della portata della divulgazione), di integrità (di cui si valuterà quanto le alterazione possano essere pregiudizievoli per l'individuo), di disponibilità (in cui diventa rilevante il fatto che sia una perdita temporanea o permanente), oppure da circostanze di violazione provocata da intenzioni malevole (fattore che aumenta sempre la probabilità che i dati vengano utilizzati in modo dannoso).

CONTESTO DEL TRATTAMENTO	
Classe dei dati violati	*Punteggio di base **
Dati semplici	1
Dati comportamentali	2
Dati finanziari	3
Dati relativi a situazione di disagio economico-sociale	3,5
Dati particolari	4

FACILITA' DI IDENTIFICAZIONE	
Livello identificabilità	*Moltiplicatore*
Trascurabile	0,25
Limitato	0,5
Significativo	0,75
Massimo	1

CIRCOSTANZE DELLA VIOLAZIONE	
Circostanza	*Correzione*
Perdita di riservatezza	Da+0a+0.50
Perdita di integrità	Da+0a+0.50
Perdita di disponibilità	Da+0a+0.50
Intenzioni malevole	+0.50

** Il punteggio di base rientrerà sempre in un valore da 1 a 4, a seconda delle successive correzioni. Ad es. a dati semplici potrebbe essere attribuito un punteggio di base = 4 qualora a causa di determinate caratteristiche dell'individuo l'informazione possa essere critica per la loro sicurezza personale o per le condizioni fisiche/psicologiche. Analogamente, anche a dati sensibili potrebbe essere attribuito un punteggio di base = 1, quando la natura dei dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo.*

Utilizzando i criteri sopra esposti, può essere calcolata quindi la gravità di una violazione di dati personali attraverso la formula

Gravità = (Contesto x Facilità di identificazione) + Circostanze

valutando infine il risultato ottenuto secondo quanto riportato nella seguente tabella

GRAVITA'	RISCHIO	DESCRIZIONE
Minore di 2	Basso	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti che supereranno senza alcun problema (tempo passato a reinserire informazioni, fastidio, irritazione, etc.)
Compreso tra 2 e 3	Medio	Gli interessati potranno incontrare inconvenienti significativi che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, etc.)
Compreso tra 3 e 4	Alto	Gli interessati potranno incontrare conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione, peggioramento della salute, etc.)
Maggiore di 4	Molto alto	Gli interessati potranno incontrare conseguenze significative o addirittura irreversibili che non potranno superare (difficoltà finanziarie come debito sostanziale o incapacità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, etc.)

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.
Le informazioni di cui agli articoli 13 e 14 del GDPR sono fornite mediante predisposizione di idonea pagina web sul sito istituzionale. Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del Comune è predisposta apposita informativa.

Il Comune agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22 del GDPR.
L'ente 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, l'ente 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, l'ente può addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
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 l'ente 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.

ALLEGATO: FINALITÀ 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, etc.);
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, etc. (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, etc.);
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 e 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 e 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, etc. 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, etc.;
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 etc.);
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 etc.) 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 dell'ente, 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 conformità 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, etc.;
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.