PROGETTO TECNICO ESECUTIVO
Dell’incarico di DPO per il Comune di Oristano

STUDIO LEGALE AVVOCATO ALESSANDRA SEBASTIANA ETZO

TITOLO DELL'INTERVENTO
Attività di DPO Comune di Oristano

a) *Organizzazione gestionale*

Un sistema di gestione e controllo dei dati, sostanziale e strettamente interconnesso alle attività dell'organizzazione, costituisce un efficace strumento nell'attività di protezione dei dati personali, nella loro valorizzazione e nella tutela dell'intero del patrimonio informativo.

Alle organizzazioni spetta l'onere di dimostrare la propria diligenza perseguendo gli obiettivi di conformità normativa su base autonoma, responsabile e documentata attraverso l'implementazione di un complesso di misure di sicurezza in grado di proteggere, nel tempo, i dati personali.

In più occasioni è stato osservato che, nel confronto con le responsabilità richieste dalle nuove norme europee, il corretto atteggiamento deve essere sostanziale e pragmatico, lontano dall'adempimento documentale formale, rigido e burocratico.

Ciò comporta, indubbiamente, uno sforzo ulteriore rispetto al passato, soprattutto per le organizzazioni meno abituate alle norme di matrice europea. I principi del Regolamento UE 679/2016 (GDPR) devono tradursi in prassi operative, controlli e comportamenti efficaci, assumendosi la responsabilità delle scelte.

Il percorso all'interno dell'organizzazione non è certo agile, per cui è importante la condivisione e la visione comune prospettica del cambiamento necessario, che incontra spesso ostacoli e resistenze.

Questa è forse la difficoltà maggiore nella definizione e nell'implementazione di tale tipologia di sistema di gestione dinamico rispetto a progetti "statici" di conformità alle norme in materia di protezione di dati personali. Nel secondo caso tipicamente le uniche funzioni coinvolte sono quelle regolamentari, le attività non sono quasi mai ricorsive e non è necessario testare l'efficacia di una soluzione individuata finché non succede qualcosa che ne dimostra l'inadeguatezza; nel primo caso, invece, le funzioni coinvolte sono tutte, le attività svolte sono ricorsive e reiterate con una frequenza dettata da eventi endogeni o esogeni e le soluzioni individuate vengono testate ricorsivamente attraverso il loro utilizzo.

Si tratta dell'oramai noto principio di "accountability": gli Enti devono saper progettare e implementare misure di sicurezza pertinenti alla propria realtà organizzativa, ai rischi connessi al trattamento, funzionali agli obiettivi di protezione dei dati e del rispetto del Regolamento.

Il modello organizzativo deve essere efficiente e flessibile, un vero e proprio strumento operativo in grado di sostenere l'impianto di protezione dei dati e rappresentare adeguatamente, alle autorità ed alle parti interessate, le capacità e l'attitudine dell'intera organizzazione alla valorizzazione e tutela del patrimonio informativo.

La discrezionalità offerta dal principio di responsabilizzazione rappresenta una preziosa opportunità che può essere colta attraverso la scelta, libera e consapevole, di un modello di gestione attinente alle reali esigenze organizzative ed alla complessità dei trattamenti. Un sistema di gestione rientra di sicuro tra queste opzioni.

Un sistema è inteso come insieme delle procedure e dei processi organizzativi funzionali al soddisfacimento di requisiti definiti. È uno strumento di carattere organizzativo e gestionale utilizzato per rispettare, in modo visibile e dimostrabile, i criteri ed i requisiti della previsti dalla norma di riferimento. Presenta fisiologiche caratteristiche di dinamicità, flessibilità e capacità di miglioramento.

Ecco quindi per punti la proposta per avere un approccio utile a costruire e governare un sistema di gestione della privacy, così da garantire costantemente una prova dell'adempimento degli obblighi privacy".

Innanzitutto, il metodo che si utilizzerà nello sviluppo e attuazione del sistema di gestione è quello circolare del Plan-Do-Check-Act (Pianificazione-Esecuzione-Controllo-Correzione e miglioramento, o Ciclo di Deming), che assicura il monitoraggio ed il miglioramento continuo dei processi e delle procedure.
Il metodo prevede che il sistema sia pianificato, implementato, controllato. I risultati dei controlli (es risultati di audit periodici) saranno valutati e costituiranno azione di miglioramento, attraverso, ove necessario, il ritorno al tavolo della pianificazione.
Applicato alla protezione dei dati personali diventa prassi di miglioramento delle modalità di trattamento dei dati, delle misure di sicurezza e dello stesso sistema di gestione privacy.
Una sorta di circolo virtuoso che si addice perfettamente ai requisiti dell'articolo 32 del GDPR dove sono richieste "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".
La Pianificazione viene eseguita sulla base della determinazione dei fattori esterni ed interni pertinenti alle finalità di interesse pubblico perseguite dall'Ente, che influenzano la sua capacità di conseguire gli esiti previsti per il proprio sistema di gestione per la sicurezza, ovvero sulla base dell'analisi del contesto interno ed esterno del Comune. Per la Pianificazione è necessaria la comprensione delle necessità e le aspettative delle parti interessate: massimamente gli uffici e gli interessati del trattamento di dati. Essa si realizza attraverso una fase di valutazione dell'insieme dei trattamenti di dati personali eseguiti dagli Enti locali, nonché degli strumenti hardware e software utilizzati dagli Enti per il loro trattamento, nonché delle politiche che regolano l'operatività dei processi. Il fine è quello di ottenere una descrizione dettagliata di tutti i processi valutabili previsti dal Regolamento comprese le infrastrutture IT (es: reti informatiche, sito web), gli archivi e le metodologie di interconnessione che ne regolano l'interoperabilità.
In fase di Esecuzione del sistema di gestione si procede con il potenziamento e rafforzamento del Gruppo di lavoro privacy. Nel tenere conto della particolare natura, delle finalità, del contesto del trattamento e dei particolari rischi per i diritti e le libertà degli interessati di essi da parte dei Titolari, essi vengono supportati mediante l'elaborazione delle evidenze dei trattamenti svolti dagli uffici, le valutazioni dei rischi inerenti i trattamenti, l'adozione delle politiche interne e procedure di gestione delle violazioni, dell'esercizio dei diritti e delle risposte agli interessati, di gestione dei fornitori, della revisione ed aggiornamento delle misure tecniche e organizzative adottate, con predisposizione della documentazione relativa, nonché attraverso la sensibilizzazione e la formazione degli operatori e del personale.
In fase di Controllo vengono valutate: la puntuale applicazione delle politiche e procedure interne; i Registri e i documenti utilizzati per la mappatura dei trattamenti; informative, e altri documenti privacy; qualità dei dati detenuti dagli uffici, contratti e altri atti con cui sono stati assunti impegni di Contitolarità, designati responsabili ex art. 28; designati gli autorizzati al trattamento e relative istruzioni.
L'attività di controllo del sistema viene condotta principalmente con lo strumento dell'Audit.
Lo schema utilizzato sarà l'ISDP 10003, unico schema nazionale attualmente accreditato per verificare la conformità al GDPR degli adempimenti messi in campo da un Titolare del trattamento.
Sono quindi presi in esame: i risultati di audit privacy precedenti; i risultati della valutazione dei rischi; i risultati delle valutazioni di impatto; le registrazioni riferite alle violazioni dei dati personali, notificate o meno; le segnalazioni di non conformità; i reclami degli interessati ed azioni di esercizio dei diritti; i risultati delle attività di revisione ed aggiornamento delle misure di sicurezza e le valutazioni riguardo i controlli effettuati; la valutazione delle segnalazioni ricevute, interne ed esterne all'organizzazione; i nuovi pareri, opinioni, linee guida ed emanazioni delle autorità.
In fase di Correzione e Miglioramento si documentano innanzitutto i rilievi analizzandone le cause, si stabiliscono e mettono in atto le azioni correttive anche di concerto con il Gruppo di Lavoro e gli uffici interessati, si rivaluta l'efficacia dell'azione correttiva a distanza di circa un trimestre.

Il miglioramento è documentato attraverso un Piano di miglioramento, che raccoglie le azioni da intraprendere, la relativa tempistica, l'impiego di risorse, i costi, le responsabilità e le altre valutazioni del caso allo scopo di risolvere le criticità rilevate in fase di monitoraggio, affinché ne siano eliminate le cause e non se ne ripresentino le condizioni.
Le azioni correttive che risultano dal piano di miglioramento elaborato servono ad rivedere ed aggiornare i processi e le modalità trattamento, tra cui l'applicazione dei principi e la scelta delle corrette basi giuridiche, i criteri precedentemente pianificati, le valutazioni del rischio di impatto (l'applicazione di misure di sicurezza rafforzate modificherà i parametri di vulnerabilità alle minacce), le procedure e le istruzioni di trattamento, la distribuzione delle responsabilità, le modalità di risposta ai diritti degli interessati.

b) ***analisi dello stato attuale e rilevazione dell'impianto privacy esistente*** **nel Comune di Oristano.**
La costruzione di un percorso di adeguamento che possa essere considerato idoneo e che possa rispettare i principi normativi i rappresenta un procedimento complesso, che richiede diverse attività e valutazioni, le quali dovranno essere svolte tenendo conto degli obiettivi di tutela e protezione del dato nonché della complessità nella quale si opera.
Pertanto, ci si propone di condurre l'analisi e rilevazione dell'impianto privacy esistente secondo step che rispondono alla logica della Due Diligence e Gap Analysis.
1) Preliminarmente:
- acquisizione della pianta organica e, se opportuno, richiesta di documenti;
- individuazione dei soggetti da interpellare in aggiunta ai referenti per ogni Ente con la calendarizzazione;
- esecuzione delle interviste per la raccolta delle informazioni necessarie per individuare i flussi di dati personali.

2) Fase di mappatura:
- Suddividere i trattamenti per ciascuna funzione/settore/ufficio; tale attività consente, tendenzialmente, di definire l'ambito dei trattamenti cui i dipendenti di una determinata area sono autorizzati;
- Inserire tutte le informazioni necessarie per la compilazione/implementazione del registro del trattamento ai sensi dell'art. 30 comma 1 GDPR;
- All'esito della mappatura dei trattamenti è possibile individuare le aree a maggiore rischio privacy;
- La mappatura dei trattamenti e dei rischi risponde a due principi: Accountability e Based approach risk;

3) Due Diligence e Gap Analysis:
- A seguito della conclusione delle interviste e della mappatura dei trattamenti dei dati personali e dei correlati rischi, si dovrà eseguire una due diligence con la relativa gap analisys;
- Nella due diligence saranno indicati: lo stato di adeguamento alla privacy dei Titolari e le irregolarità riscontrate (gap analysis); gli adempimenti da eseguire per la compliant privacy; la tempistica da decidere a seconda del livello di rischiosità dei trattamenti individuati (risk based approach); le eventuali ulteriori soluzioni utili ai fini dell'accountability.

c) ***valutazione dello stato attuale del modello di gestione, privacy e data protection*** **adottato.**
A seguire, e sulla base delle caratteristiche di ogni ente, del suo grado di autonomia e degli aspetti critici emersi nella fase iniziale, la fase di valutazione comprende le seguenti attività:
a. Macroanalisi dei flussi informativi legata al trattamento dei dati e supporto al referente di ogni ente nella mappatura dei processi;
b. Supporto alla compilazione del registro dei trattamenti di dati personali e del registro delle categorie di attività con validazione finale;

c. Interventi formativi collettivi per i referenti degli enti;
d. Valutazione delle vulnerabilità;
e. Assistenza nella compilazione delle DPIA;
f. Valutazione degli scostamenti dagli obblighi normativi;
g. Elaborazione del piano di adeguamento complessivo, contenente le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi esterni (se necessario) e dei tempi previsti.
In fase di sviluppo del sistema di gestione privacy si interverrà sui seguenti contenuti:

- Nomine dei responsabili;
- Nomina degli autorizzati art. 2 quaterdecies Codice;
- Accordi contitolari del trattamento;
- Nomine delegati interni;
- Costituzione/implementazione team privacy;
- Predisposizione del registro del titolare dei trattamenti (30,1);
- Predisposizione del registro del responsabile del trattamento (qualora si trattino dati anche da responsabile e non solo da titolare) 30.2;
- Data Breach policy ART. 33;
- Procedura per la soddisfazione dei diritti degli interessati;
- Retention policy;
- DPIA (valutazione di impatto e rischio del trattamento dati effettuato) ART. 35 e ss.;
- Regolamento di utilizzo degli strumenti informatici Linee Guida del Garante del 2007;
- Compliance sito web.

Le attività relative a questa fase verranno svolte da remoto e presso l'Ente, quando necessario

Modalità con cui si intende garantire l'integrazione con i servizi e le attività istituzionali e organizzative del Comune.
Per l'esecuzione delle attività sopra descritte, a partire dalla fase iniziale, l'Ente ha già nominato un referente, soggetto che caratterizzato da un'ampia visione delle articolazioni del Comune e delle attività svolte all'interno.
Si verificherà la disponibilità ed eventualmente si procederà a implementare il gruppo di lavoro privacy che risulta già attivo. I partecipanti forniranno informazioni sulla struttura organizzativa dell'Ente e sulle modalità con cui quest'ultimo svolge la propria attività per consentire di individuare le tipologie di dati trattati e le categorie di attività di trattamento; il GDL ha il compito di coinvolgere ed interagire con il DPO per permettergli di svolgere la propria attività e così di intervenire sin dalle prime fasi della progettazione in attività che implichino il trattamento di dati personali (privacy by design), al fine di supportare il Titolare nella stesura della documentazione conforme alle disposizioni vigenti (es: atti di gara, disciplinari, informative, contratti).
Particolare attenzione verrà data ai servizi svolti in forma associata e/o con la determinazione congiunta di finalità e mezzi di trattamento anche con Enti terzi, al fine della corretta determinazione di obblighi e responsabilità, con assistenza nella stesura per esempio di accordi di contitolarità ai sensi dell'art. 26 del GDPR.
In particolare il GDL sarà chiamato a descrivere, sotto la supervisione del DPO e con gli strumenti contemplati nelle fasi precedenti, contando anche sul supporto degli amministratori di sistema, la mappatura dei processi per individuare quelli collegati al trattamento dei dati personali e alla compilazione del registro delle attività di trattamento e del registro delle categorie di attività trattate da ciascun Responsabile.
L'attività di DPO verrà svolta ordinariamente presso il Comune, che metterà a disposizione la propria sede

e gli strumenti necessari alla esecuzione dei tavoli di lavoro e coordinamento tra il DPO e i referenti dei singoli uffici, incontri svolti con frequenza almeno mensile e della durata minima di una mezza giornata. Sulla base di un calendario concordato con i referenti degli uffici, saranno previste visite periodiche programmate presso le diverse sedi per la verifica della corretta adozione del modello di funzionamento della protezione dei dati oltre a quelle necessarie in seguito a fatti straordinari quali, a titolo meramente semplificativo, eventi di *data breach*, visite ispettive, cambiamenti sostanziali della struttura organizzativa.
Il DPO, promuovendo anche tavoli tecnici tematici o gruppi di lavoro per settore, darà priorità all'adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni o stesura ex novo della documentazione e avvio della relativa adozione da parte dell'Ente.
Con il potenziamento del Gruppo di lavoro e delle relazioni tra DPO e referenti si garantisce l'interazione costante e con i servizi e le attività istituzionali e organizzative del comune, oltre che il rispetto del principio di accountability in termini di autoresponsabilizzazione, alla base del Reg. U.E 679/2016.

Formazione del personale
Al fine di erogare personalmente la formazione obbligatoria prevista dagli artt. 29, 32 e 39 del GDPR e l'addestramento ai responsabili e al titolare del trattamento e a tutti i dipendenti del Comune, destinatari dei servizi, si propone il seguente programma didattico con indicazione delle modalità di erogazione dei singoli moduli su base annuale, per la formazione ed aggiornamento degli operatori, sulle problematiche e la legislazione concernente la materia del trattamento dei dati. Resta inteso che diversi modalità, contenuti ovvero l'ordine di trattazione, potranno essere diversamente concordati con il Referente e il GDL.
Il programma seguente tiene conto dei contenuti formativi eventualmente già svolti dall'Enete tra il 2018 ed il 2020 e che, per estrema sintesi, potrebbero aver riguardato: Il nuovo quadro normativo in materia di protezione dei dati personali; Principi generali e Definizioni; Soggetti; Gli Obblighi del Titolare; Misure di Sicurezza; Gestione delle violazioni; Responsabilità e Sanzioni; Rapporti tra Privacy, Trasparenza e Pubblicità.
Resta inteso che qualora dovesse risultare necessario integrare sui predetti argomenti, si manifesta fina da ora la disponibilità a riprendere tali contenuti.
Primo anno
Modulo 1: 4 ore in presenza
Il Registro delle attività di trattamento: cos'è e come si realizza.

- La costruzione di un registro in una PA, in particolare per attività connesse a obblighi di legge;
- Alcune indicazioni operative;
- L'aggiornamento dei Registri;
- Esempi e buone prassi;
- La cooperazione con l'Autorità di controllo (Art. 31 del GDPR).

I diritti degli interessati:

- La disciplina dei diritti degli interessati contenuta nel GDPR;
- Gli obblighi del titolare;
- I soggetti coinvolti;
- Il ruolo del DPO;
- Gli strumenti di tutela;
- Procedure di gestione, risposta e modulistica;
- Esempi e buone prassi.

Modulo 2: 4 ore in presenza
La sicurezza dei dati personali secondo il GDPR.

- Misure tecniche e organizzative adeguate (indicazioni operative; concetti fondamentali;
- Il rischio per la sicurezza vs. rischio per la protezione dati; il manuale ENISA per la valutazione del

rischio sicurezza)
- Il concetto di rischio del GDPR e gli strumenti utili alla sua valutazione.
- Come si effettua una valutazione del rischio: il supporto del DPO
- La valutazione d'impatto sulla protezione dei dati personali: istruzioni per l'uso
- La consultazione preventiva del Garante sugli atti legislativi e le misure regolamentari, nell'ambito della valutazione di impatto e sui trattamenti a rischio elevato in ambito pubblico. Il ruolo del DPO;
- Esempi e buone prassi.

Secondo anno
Modulo 3: 4 ore in presenza
Le categorie particolari di dati personali; i motivi di interesse pubblico rilevante, il regime dei dati biometrici, genetici e relativi alla salute; il trattamento dei dati personali relativi a condanne penali e reati, nel regolamento e nel quadro normativo di riferimento
- Premessa. Le categorie particolari di dati personali
- Il divieto e le specifiche deroghe per il trattamento
- I motivi di interesse pubblico rilevante (Il precedente sistema di garanzie previsto dal Codice: I regolamenti per i trattamenti dei dati sensibili e giudiziari)
- Il regime dei dati biometrici, genetici e relativi alla salute
- Il sistema di garanzie del nuovo Codice: a) Le misure di garanzia, b)Le regole deontologiche, c) dalle autorizzazioni generali al provvedimento prescrittivo di carattere generale (art. 21 del d.lgs n.101 del 2018)
- Il trattamento dei dati personali relativi a condanne penali e reati
- Esempi e buone prassi.

Modulo 4: 4 ore in presenza
La base giuridica del trattamento in ambito pubblico e il ruolo del Garante nell'applicazione della normativa.
- Lo scenario del trattamento dei dati in ambito pubblico
- La base giuridica del trattamento
- Le condizioni necessarie per trattare i dati particolari
- I trattamenti automatizzati e la profilazione
- Il ruolo del DPO
- Il ruolo del Garante nella regolazione dei trattamenti pubblici
- Esempi e buone prassi.

Terzo anno
Modulo 5: 4 ore in presenza
Contitolari, Responsabili e autorizzati in ambito pubblico
- Accordi di contitolarità (Art. 26 GDPR)
- Contratti e altri atti giuridicamente vincolanti (Art. 28 GDPR)
- Istruzioni (Art. 29 GDPR)
- Esempi e buone prassi

I flussi internazionali di dati.
- Il trasferimento dei dati personali verso Paesi terzi e organismi internazionali
- Piattaforme e Cloud per la PA
- Linee guida Agid
- Esempi e buone prassi

Modulo 6: 4 ore in presenza
Il ruolo del Garante nell'applicazione della normativa in materia di protezione dei dati personali. Attività istruttoria, ispettiva, responsabilità e sanzioni amministrative.

- L'Autorità
- Quale ruolo per l'Autorità
- Compiti e poteri
- Attività istruttoria
- Attività ispettiva
- Le responsabilità
- I procedimenti correttivo sanzionatori
- Le sanzioni amministrative
- Esempi e buone prassi.

Per ogni modulo viene predisposto un test di apprendimento a risposta multipla chiusa, con attribuzione di un punteggio finale e di un punteggio minimo per il superamento del test.
In ogni modulo viene dedicata un'ora alle domande/risposte e somministrazione del test di apprendimento, per consolidare e verificare il livello di acquisizione dei concetti oggetto della formazione.
I test verranno corretti a cura del DPO e verrà predisposto un report delle risultanze con indicazione dei soggetti che dovranno ripetere il test per non aver raggiunto il punteggio minimo.
Delle attività di formazione viene data evidenza in una relazione che documenta lo svolgimento delle singole attività, cui sono allegati i fogli presenza con le firme dei partecipanti in entrata e uscita, i report e i test, oltre che il materiale didattico, ai fini della eventuale richiesta di esibizione e dimostrazione dell'osservanza degli obblighi di formazione da parte del Titolare.
La predetta proposta formativa viene integrata mediante l'impegno a segnalare ai referenti e personale dei vari uffci la possibilità di iscrizione a webinar su tematiche specifiche nella materia dei dati personali, erogati dall'Autorità Garante, Federprivacy e/o altre primarie istituzioni operative nel settore della *data protection,* per il tramite di esperti della materia di livello nazionale ed internazionale.
Resta inteso che i moduli potranno essere erogati, in accordo con Referente e GDL, in modalità streaming, qualora per ragioni di forza maggiore (es: divieto di assembramenti/seminari causa Covid) o per comodità, si preferisca non tenerli in presenza.

Proposte migliorative, funzionali e strutturali, e altre risorse strumentali destinate alla realizzazione del progetto di gestione dei servizi che permettano il raggiungimento degli obiettivi di adeguamento e corretta gestione dei processi, adempimenti e criticità degli enti aderenti al sistema che l'operatore economico propone di attivare e proporre per migliorare la qualità dei servizi.

L'esperienza pregressa presso Enti Locali, ha visto l'elaborazione di schemi di regolamentazione delle procedure di gestione di risposta agli interessati per l'esercizio dei diritti, di regolamentazione dei sistemi di videosorveglianza con aggiornamento delle relative informative e cartelli, di procedure di gestione delle violazioni (*data breach*) coi relativi registri.
Si tratta di regolamenti la cui adozione è caldeggiata in diversi provvedimenti dell'Autorità Garante.
Le proposte migliorative che quivi si formulano vanno anche oltre i suggerimenti delle Autorità e si pongono in continuità, valorizzando il lavoro finora svolto dal Comune.
Esse riguardano la progressione di tutti verso forme di regolamentazione sempre più specifiche e in grado di offrire un valido supporto ai singoli operatori nell'applicazione pratica dei principi della normativa in materia di protezione dei dati personali.

Si comincerà con la creazione di uno schema di regolamento che disciplini e fornisca un quadro organico e coordinato dei profili applicativi relativi alle tre tipologie di accesso: civico, generalizzato e documentale, con il fine di dare attuazione al nuovo principio di trasparenza introdotto dal legislatore e di evitare comportamenti disomogenei tra uffici della stessa amministrazione.
L'adozione di un regolamento sulle forme di accesso, prevedendo le casistiche di accesso in cui vi sono dati personali, assolve la duplice funzione di rappresentare una istruzione specifica che l'Ente da ai propri autorizzati al trattamento di dati, responsabilizzandoli di conseguenza al rispetto delle disposizioni, ma anche alla funzione di dare evidenza e documentare i processi valutativi e di bilanciamento di contrapposti interessi/diritti che ha svolto ogni Titolare di trattamento. Si garantisce così la piena rispondenza a quanto richiesto dal GDPR (così come è con l'adozione degli altri menzionati regolamenti e procedure interne).
A seguire, sulla base delle attività di mappatura svolte nei vari settori/uffici verrà implementata una procedura di gestione condivisa che possa garantire misure di garanzia e protezione massime per particolari categorie di dati personali (art. 9 e art. 10 del GDPR), nonché per particolari categorie di interessati (es: minori, persone in stato di disagio economico e/o sociale, portatori di handicap).
Nella stessa ottica, si aggiunge come offerta migliorativa anche l'attività di aggiornamento e revisione dei regolamenti già in essere.
L'offerta migliorativa viene integrata anche dall'invio con cadenza almeno mensile all'indirizzo dei referenti e al protocollo di una nota di aggiornamento sui principali provvedimenti normativi, amministrativi e sanzionatori adottati dalle Autorità competenti (es: Autorità Garante Privacy italiana, Comitato dei Garanti Europei, Corti nazionali ed internazionali) nelle materie di interesse nel particolare settore della pubblica amministrazione, con riferimento specifico al comparto degli Enti Locali.
Infine si dichiara la disponibilità a ripetere gli incontri formativi svolti per i nuovi assunti.

Firma del Legale rappresentante
(sottoscrizione digitale)

……

Firmato digitalmente da: Alessandra Sebastiana Etzo
Data: 10/05/2022 13:25:39