COMUNE DI RHO

Area 1 - Affari generali, Personale e Organizzazione

MODELLO ORGANIZZATIVO

IN MATERIA DI PROTEZIONE DEI DATI

PERSONALI

(Regolamento UE 2016/679)

1. INTRODUZIONE

Il 25 maggio 2018 è divenuto ufficialmente operativo il nuovo Regolamento generale europeo in materia di protezione dei dati personali, definito – anche nel prosieguo del presente documento - GDPR, acronimo di "General Data Protection Regulation".
Il nuovo Regolamento costituisce, insieme alla Direttiva (UE) n. 2016/680, il "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea al fine di rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini comunitari.

Il nuovo apparato normativo si basa su un nuovo assioma di fondamentale importanza: la responsabilizzazione, ovvero nell'accezione inglese, il principio di *accountability*.
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.
Al Titolare viene affidato, altresì, 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 questi 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 in cui il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Spetta dunque al Titolare mettere in atto una serie di misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.

Le principali novità introdotte dal GDPR, possono essere così sintetizzate:

- è introdotta la responsabilità diretta del Titolare del trattamento in merito al compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali;
- è definita la nuova categoria di dati personali (i c.d. dati sensibili di cui al precedente Codice Privacy);
- viene istituita la figura obbligatoria del Responsabile della Protezione dei Dati (DPO), incaricato di assicurare una gestione corretta dei dati personali negli Enti;
- viene introdotto il Registro delle attività del trattamento ove sono descritti i trattamenti effettuati e le procedure adottate dall'Ente; il Registro dovrà contenere specifici dati indicati dal GDPR;
- viene richiesto agli Enti l'obbligo, prima di procedere al trattamento, di effettuare una valutazione di impatto sulla protezione dei dati; tale adempimento è richiesto quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Con il D. Lgs. 10 agosto 2018, n. 101 pubblicato sulla GURI del 4/9/2018 ed entrato in vigore il 19/9/2018, sono state approvate le "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento europeo (UE) 2016/679, relativo alla protezione delle persone fisiche con riferimento ai dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dati)*". Con tale decreto, che in parte abroga, modifica e novella profondamente il precedente decreto n. 196/2003, si completa il quadro della disciplina normativa nella materia in oggetto, andando a costituire il nuovo "Codice Privacy".

È importante sottolineare che la disciplina nazionale integra quella europea e le disposizioni nazionali sono da ritenersi legittime in quanto e nella misura in cui:

- rientrino nelle materie rimesse dal GDPR al legislatore nazionale;

- il loro contenuto sia conforme alle disposizioni del GDPR;
- esse siano interpretate e applicate nel rispetto del Regolamento.

La normativa italiana e quella europea costituiscono, dunque, un ordinamento giuridico integrato e complesso, retto dal principio di supremazia della normativa europea su quella nazionale.

2. IL PERCHÉ DI UN MODELLO ORGANIZZATIVO

L'adeguamento al Regolamento UE 2016/679 impone al Titolare del trattamento di prestare grande attenzione al fattore organizzativo. 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 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, di sistemi mirati per un'applicazione "ordinata" e completa della normativa sui trattamenti di dati personali. Tale logica di costruzione di un modello *ad hoc* è simile, peraltro, a quella prevista in materia di prevenzione della corruzione.

Il modello organizzativo di cui al presente documento individua quindi le politiche, gli obiettivi strategici e gli standard di sicurezza messi in atto dal Comune di Rho 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 di gestione della privacy adottato dall'Ente dovrà essere sottoposto a costante monitoraggio da parte dell'Amministrazione comunale, allo scopo di intervenire rapidamente sull'assetto organizzativo, anche su proposta del DPO, in caso di modifiche normative, a seguito dell'evoluzione tecnologica ovvero per la necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali.
Il presente modello organizzativo, quindi, sarà sottoposto a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

3. NORME E PRINCIPI GENERALI

Il Comune di Rho 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. Il Comune di Rho assicura in particolare che, nello svolgimento dei compiti e funzioni istituzionali, i dati personali siano trattati nel rispetto della legislazione vigente e dei seguenti principi:

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

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

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

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

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

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

h) "*responsabilizzazione*": il Titolare del trattamento è competente per il rispetto dei principi imposti dal GDPR e deve essere in grado di comprovarlo.

4. SENSIBILIZZAZIONE E FORMAZIONE

La tutela della privacy è da considerare non solo come un oneroso rispetto di adempimenti burocratici ma, soprattutto, come garanzia per il cittadino che si rivolge alla Pubblica Amministrazione, di una riservatezza totale dal punto di vista reale e sostanziale.
Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Comune di Rho 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.
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 periodicamente, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.
La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Comune.

5. 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, nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo.
Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati ed autorizzati. Non è consentito il trattamento da parte di persone non puntualmente autorizzate ed istruite in tal senso.
Al fine di garantire la correttezza delle operazioni di trattamento, il Comune provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti svolti, finalizzata alla compilazione ed aggiornamento del Registro delle attività di trattamento di cui al successivo punto 18.

6. TIPOLOGIA DI TRATTAMENTI

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

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

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

7. LE FIGURE DI RIFERIMENTO

Il GDPR ridisegna il ruolo, i compiti e le responsabilità del Titolare e delle altre figure previste per il trattamento dei dati personali, in relazione ai nuovi principi e strumenti introdotti dallo stesso e individua la nuova figura del Responsabile della protezione dei dati.

8. IL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento di dati personali, ai sensi degli artt. 4, 7 e 24 del Regolamento, è l'Ente (nella persona del suo Legale rappresentante), cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire - ed essere in grado di dimostrare - che il trattamento è effettuato conformemente al Regolamento.

Spetta, in particolare, al Titolare:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi necessari per la protezione dei dati personali;
- designare il Responsabile della protezione dei dati;
- designare i soggetti ai quali è affidata l'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
- effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il Responsabile della protezione dati designato;
- assicurare l'adeguata istruzione dei soggetti designati e autorizzati al trattamento dei

dati personali.

Il Sindaco, in quanto legale rappresentante dell'Ente, riveste la figura di Titolare del trattamento.

Il Sindaco designa i dirigenti, ciascuno per il proprio ambito di competenza, quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti dei dati personali effettuati dall'Ente in esecuzione del Regolamento e del "Codice".

Relativamente ai trattamenti dei dati personali gestiti da più strutture in modo trasversale, si applica il criterio della prevalenza.

Il Sindaco designa altresì il Responsabile (esterno) della protezione dati.

9. I DESIGNATI AL TRATTAMENTO

In attuazione del D. Lgs. n. 196/2003, nel testo previgente all'adeguamento al GDPR, i Dirigenti erano stati individuati, come da nomine in atti, Responsabili del trattamento dei dati nell'ambito delle rispettive funzioni di competenza.
L'articolo 28 del GDPR ha definito il Responsabile del trattamento come il soggetto che effettua il trattamento "per conto del Titolare". In forza del rapporto di immedesimazione organica che intercorre tra i Dirigenti ed il Titolare, non risulta configurabile un rapporto di rappresentanza da parte di questi "per conto del Titolare".
In considerazione dell'entrata in vigore della nuova normativa del GDPR e della modificata definizione di Responsabile del trattamento, si rende necessario procedere all'adeguamento degli atti di nomina dei Dirigenti al fine di attribuire ai medesimi, in qualità di soggetti appositamente designati, specifiche funzioni e compiti connessi al trattamento dei dati personali, ancorché non più identificabili come Responsabili del trattamento.

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

Questa Amministrazione ritiene dunque che i Dirigenti debbano conseguentemente essere autorizzati al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione.

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

10. 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 GDPR e la normativa nazionale di adeguamento, consentono dunque di mantenere le funzioni ed i compiti assegnati a figure interne all'Ente che, ai sensi del Codice nel testo previgente all'adeguamento al GDPR - ma non anche ai sensi del GDPR - potevano essere definiti come "incaricati".
Il personale operante (a qualunque titolo ed a qualunque livello) all'interno del Comune è conseguentemente autorizzato – e non potrebbe essere diversamente - al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate.
Stante la complessità dell'organizzazione del Comune di Rho, in relazione al numero dei servizi e dipendenti assegnati agli stessi, si ritiene di attuare il principio in base al quale tutti i dipendenti che operano presso il Comune di Rho per documentata preposizione ad una unità organizzativa, sono autorizzati al trattamento dei dati afferenti alla stessa, che dovrà essere attuato per le finalità specifiche richieste, secondo le istruzioni che saranno impartite dal Responsabile designato, che vigilerà affinché le persone fisiche autorizzate effettuino le operazioni di trattamento nel rispetto dei principi del GDPR di cui al precedente punto 3.
La designazione si considera realizzata attraverso l'assegnazione delle risorse umane alle varie Direzioni e Servizi attuata tramite il PEG/Piano della Performance adottato annualmente ovvero tramite gli atti gestionali di trasferimento adottati in corso d'anno dalla Direzione del Personale.
Spetta ai Dirigenti individuare, nell'ambito gerarchico delle risorse assegnate, le diverse misure di responsabilità nel trattamento dei dati, anche in relazione alla valenza della gestione di particolari banche dati con specifiche esigenze di tutela.

11. IL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Sono designati Responsabili del trattamento di dati personali i soggetti esterni all'Amministrazione che siano tenuti, a seguito di convenzione, contratto, assegnazione di incarichi o altro rapporto contrattuale, ad effettuare il trattamento di dati personali per conto del Titolare. Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.
Attesa la natura negoziale della designazione dei responsabili del trattamento, questa deve essere effettuata tramite inserimento nei diversi modelli contrattuali di apposite clausole vincolanti in ordine al rispetto delle disposizioni e degli obblighi in materia di protezione dei dati personali, in aderenza ai fac-simile prodotti dall'Ente, da adattare al caso specifico.

I Responsabili del trattamento possono nominare dei sub-responsabili, purché autorizzati preventivamente. In tal caso, il Responsabile vincola il sub-responsabile con un contratto (o altro atto giuridico conforme del diritto nazionale) che contenga gli stessi obblighi previsti nel contratto tra il Responsabile e l'Ente. Il responsabile iniziale conserva nei confronti dell'Ente l'intera responsabilità degli adempimenti degli obblighi del sub-responsabile.

12. IL RESPONSABILE PROTEZIONE DATI (DATA PROTECTION OFFICER - DPO)

Il Regolamento prevede l'obbligo per il Titolare del trattamento, ove questo sia effettuato da un'Amministrazione pubblica, di designare un Responsabile della protezione dati (Data Protection Officer – nel prosieguo DPO).

Il Responsabile protezione dati ha compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento e di sorveglianza sulla corretta applicazione del Regolamento (art. 37 GDPR).

Il Responsabile protezione dati può essere individuato tra il personale dipendente in organico oppure può essere affidato all'esterno in base ad un contratto di servizio. Con proprio decreto n. 3 del 23.05.2018, il Sindaco ha designato quale DPO per il Comune di Rho, il Segretario generale, dott. Matteo Bottari.

I relativi dati di contatto sono stati comunicati al Garante per la protezione dei dati personali e sono pubblicati sul sito internet dell'Ente.

I compiti assegnati al DPO, in aderenza agli artt. 37 e s.s. del DGPR, conformati all'organizzazione dell'Ente sono i seguenti:

- informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto del gruppo dei referenti designati dalle strutture;
- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente 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;
- coopera con il Garante per la protezione dei dati personali;
- funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del servizio ICT competente o ne richiede di specifiche;
- promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
- partecipa alla gestione degli incidEnti di sicurezza nelle modalità previste da specifica policy dell'Ente;
- formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento;
- fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato nel paragrafo che segue.

13. PARERI DEL RESPONSABILE PROTEZIONE DATI

Il Responsabile protezione dati fornisce il proprio parere – che può essere obbligatorio o facoltativo - in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano nei casi di seguito indicati.

❖ *Pareri obbligatori*

Devono essere obbligatoriamente richiesti pareri in ordine a:

- individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della riservatezza,

integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di incidenti di sicurezza o analisi dei rischi;

- adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici o regolamenti con impatto sulla sicurezza delle informazioni;
- individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- incidenti sicurezza.

❖ ***Pareri facoltativi***

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

- progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;
- valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;
- valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis del D.Lgs. 14 marzo 2013, n. 33 e, in via generale, del Regolamento UE n. 679/2016;
- opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere devono essere inviate al seguente indirizzo di posta elettronica: rdp.privacy@comune.rho.mi.it e per conoscenza al dirigente incaricato della tenuta del registro e al dirigente della struttura competente in materia di Sistemi informativi. Possono presentare le richieste di parere i Dirigenti designati relativamente alla disciplina di trattamento dati nelle materie di rispettiva competenza.

I pareri sono espressi secondo le seguenti codifiche:

- NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;
- OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
- PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri "NC" e "OS" il Dirigente deve formalizzare, nelle medesime forme utilizzate dal DPO per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO.

I pareri espressi dal DPO sono conservati agli atti della struttura dirigenziale che ne ha fatto richiesta.

14. ACCESSO CIVICO GENERALIZZATO E RUOLO DPO

Il D.L. 97/2016, di modifica del D. Lgs. n. 33/2013 ha introdotto l'istituto dell'accesso

civico “generalizzato”, che attribuisce a “chiunque” il diritto di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione. L’esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall’articolo 5-bis” del d.lgs. n. 33/2013).

L’art. 5, comma 5, del D. Lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l’Amministrazione debba verificare l’eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.

Il DPO funge da supporto alle strutture competenti a richiesta sulle singole istanze di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato. In particolare, il DPO, su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all’opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.
Sulla scorta di tale parere le strutture competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell’interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

Il DPO funge altresì da supporto al RPCT nei casi di riesame di istanze di accesso negato o differito a tutela dell’interesse alla protezione dei dati personali. Nel Comune di Rho le due figure coincidono.

15. STRUTTURA COMPETENTE AI SISTEMI INFORMATIVI

Spetta alla struttura competente in materia di Sistemi informativi l’adozione di *policy* in materia di privacy e sicurezza informatica, con particolare riferimento all’utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l’evoluzione tecnica o normativa lo renda necessario; svolge, altresì, un ruolo di supporto al DPO in tema di risorse strumentali e di competenze.

La struttura è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto del principio di *accountability*, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi operativi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al GDPR da parte del DPO.

In particolare, l’ufficio ai Servizi informativi:

- individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell’Ente; tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del DPO, come, ad esempio, la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e l’aggiornamento dei disciplinari tecnici trasversali;
- condivide le evidenze dell’analisi dei rischi con il DPO, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;
- provvede, ogni qualvolta venga avvertito un problema di sicurezza a:
  - attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;
  - individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati

personali, previo parere obbligatorio del DPO;

- segnalare tempestivamente al DPO le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;

- svolge verifiche sulla puntuale osservanza della normativa e delle policy di Ente in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dallo stesso;
- promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno dell'Ente, coordinandosi con le azioni promosse dal DPO.

Al Dirigente competente in materia di Sistemi informativi spetta:

- la sottoscrizione degli atti di notifica e di consultazione preventiva al Garante;
- la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

Per quanto riguarda più in generale le misure di sicurezza informatica si rinvia ai seguenti documenti adottati dal Comune di Rho:

- "Policy di sicurezza data center del Sistema informatico del Comune di Rho",
- "Disciplinare per l'utilizzo degli strumenti informatici, della posta elettronica e di internet";
- "Manuale del Sistema di Protocollo Informatico, dei flussi documentali e degli Archivi" con particolare riferimento al "Piano per la sicurezza informatica".

16. GLI AMMINISTRATORI DEL SISTEMA INFORMATICO

Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" come modificato con successivo provvedimento datato 25/06/2009, il Comune si avvale di amministratori 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 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.
Può essere designato amministratore del sistema informatico un dipendente comunale a tempo indeterminato inquadrato almeno nella categoria "C" ovvero, nel caso di mancanza di professionalità interne, un soggetto esterno, persona fisica o giuridica.

Nell'atto di designazione ovvero nel contratto di servizio con cui è stato nominato l'Amministratore di sistema, devono essere riportati, altresì, tutti gli adempimenti 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 D. Lgs. n. 82/2004 e ss.mm.ii..

In particolare spetta agli amministratori di sistema la cura dei seguenti adempimenti:

- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza

- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi
- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up secondo i criteri stabiliti dal Titolare/Responsabile del Trattamento dei dati oppure, in caso di incarico a soggetto esterno della gestione dei backup, sovrintendere all'operato del soggetto esterno e informare Titolare e responsabili di eventuali criticità nella gestione
- assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro
- collaborare con i responsabili nel sovrintendere all'operato di eventuali tecnici esterni all'amministrazione
- fare in modo che sia prevista la disattivazione dei "codici identificati personali" (User-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore
- gestire gli account di accesso ai sistemi per tutti gli incaricati che accedono a tutti i sistemi informatici aziendali
- gestire le password di root o di amministratore di sistema
- collaborare con il responsabile del trattamento dei dati personali
- gestire dei profili di accesso ai sistemi per gli ambienti operativi in dotazione ai sistemi informatici comunali
- gestire le caselle postali con relative deleghe di ricezione/invio
- gestire i permessi di accesso alle risorse condivise (Programmi, file e stampanti)
- gestire i controlli di sicurezza legati alla navigazione Internet
- gestire i controlli di sicurezza legati alla ricezione della posta elettronica (antispam e antivirus)
- gestire l'aggiornamento dei sistemi operativi (patching) e dei sistemi di sicurezza (antivirus e antispam)
- analisi di problemi e malfunzionamenti siano dei singoli sistemi che della connettività tra sistemi ed applicazioni di proprietà dell'ente
- informare titolare e responsabili sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

All'amministratore di sistema è consentito l'accesso ai dati personali contenuti nelle banche dati dell'Ente esclusivamente e solo per il tempo necessario per garantirne il buon funzionamento. Ogni eventuale accesso a tali banche dati e archivi dovrà in ogni caso avere luogo nel rispetto delle procedure aziendali di accesso ed autenticazione.

Con decreti del Sindaco n. 1 e n. 2 del 07/01/2019 sono stati designati Amministratori di sistema del Comune di Rho i due dipendenti di cat. C assegnati al Sistema informativo comunale in veste di Analista di gestione operativa.

17. MISURE PER LA SICUREZZA DEI DATI PERSONALI

La Giunta comunale, i Dirigenti/Responsabili di P.O. e agli Amministratori di sistema informatico provvedono, per quanto di rispettiva competenza, all'adozione - e 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.

18. 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.

Il Regolamento prevede l'adozione di un "registro delle attività di trattamento", che reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, del Sindaco e/o del Dirigente designato, del DPO;
b) le finalità del trattamento;
c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

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. n. 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.

Il Comune adotta il registro in formato elettronico, che meglio può consentire l'aggiornamento e l'accesso alle informazioni. Una copia cartacea è consegnata presso il Titolare del trattamento.

Il registro è sottoposto all'approvazione della Giunta comunale, e verificato con cadenza almeno annuale, e una sua copia informatica è posta in conservazione sostitutiva.

Spetta ai Dirigenti:

- 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;
- contribuire alla tenuta del registro in relazione ai trattamenti della struttura organizzativa di competenza, fornendo le necessarie informazioni e valutazioni;
- 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.

La tenuta del registro è demandata al Direttore dell'Area Affari generali, Personale e Organizzazione, il quale coordina le attività di implementazione e aggiornamento sistematico dei dati del registro stesso coinvolgendo allo scopo i singoli Dirigenti, ai quali spetta la responsabilità sulla completezza e adeguatezza dei dati e delle misure indicate per i trattamenti di competenza.

Per lo svolgimento dei compiti di supporto assegnati connessi al GDPR, il suddetto Dirigente dovrà individuare formalmente nella organizzazione dell'Area di riferimento, l'ufficio deputato al coordinamento delle attività di protezione dei dati personali, che costituirà un riferimento per le altre strutture organizzative del Comune e per il DPO.

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 le prerogative del Responsabile della protezione dei dati personali si evince che tra le altre egli 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 assegnata 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.

19. RUOLI ORGANIZZATIVI

Viene individuato nella Conferenza dei Dirigenti di cui all'art. 13 del vigente Regolamento sull'ordinamento degli uffici e servizi del Comune di Rho, il "Comitato privacy" con il compito di garantire un maggior presidio e coinvolgimento sulla data protection a supporto del DPO, attraverso l'adeguamento uniforme dei sistemi e della gestione dei dati nelle varie unità organizzative.

Ogni dirigente, poi, individuerà dei dipendenti di idonea categoria, che costituiranno il gruppo dei referenti Privacy con il compito in particolare di:

- collaborare con i dirigenti dei Servizi di appartenenza all'attuazione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Ente;
- effettuare la ricognizione costante, a mezzo del Registro, dei trattamenti di dati personali effettuati dai Servizi di appartenenza;
- fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO;
- promuovere e collaborare al bisogno alla revisione e all'aggiornamento dei disciplinari tecnici;
- coordinare le richieste di parere al DPO dei Dirigenti dei Servizi di appartenenza nei casi e con le modalità previsti dal presente documento;
- sottoporre ai Dirigenti eventuali problematiche riscontrate nei Servizi di appartenenza che possano generare dei rischi e rendano necessario intervenire sulle modalità di gestione dei dati personali.

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

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

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

Una informativa breve è fornita, mediante idonei strumenti:

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

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

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

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

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

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

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

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

richiesta; oppure

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

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

Questa Amministrazione assicura le forme di accessibilità e trasparenza, nelle varie forme in cui la legislazione riconosce il diritto di accesso (D.Lgs. n. 267/2000, Legge n. 241/90, D. Lgs. n. 33/2013).

Nell'assicurazione le attività per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, così come più in generale gli obblighi di pubblicità e pubblicazione, 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 dall'eventuale soggetto controinteressato (in caso di accesso).

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigente, gli uffici, nel dare riscontro alle richieste di accesso ovvero nel pubblicare i provvedimenti, in linea generale dovranno 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.

ORGANIGRAMMA PRIVACY