COMUNE DI GENOVA

RESPONSABILE PROTEZIONE DATI (DPO)
Proposta di Deliberazione N. 2021-DL-319 del 21/07/2021

Approvazione del "REGOLAMENTO IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI"

Il Presidente pone in discussione la proposta della Giunta n. 55 in data 22 luglio 2021;

Su proposta dell'Assessore alla Avvocatura e Affari legali, Famiglia e relativi diritti, con delega ai "Rapporti con Consiglio Comunale, Municipi e Città Metropolitana", Avv. Lorenza Rosso;

Visti:

- Il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, di seguito "GDPR");

- Il DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";

- Il DECRETO LEGISLATIVO 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", come modificato dal citato Decreto Legislativo 10 agosto 2018, n. 101;

Richiamato, in particolare:

- l'articolo 5 del GDPR che, al paragrafo 1, enuncia i principi applicabili al trattamento dei dati personali e al paragrafo 2 pone in capo al Titolare del trattamento (d'ora in avanti, Titolare) il principio di responsabilizzazione cd. "accountability", in base al quale il medesimo deve garantire, ed essere in grado di comprovare, il rispetto di tali principi;

Rilevato che:

la responsabilizzazione del Titolare del trattamento si realizza anche mediante:

- la concreta adozione sia al momento di determinazione dei mezzi e delle modalità del trattamento, sia all'atto del trattamento stesso di misure tecniche ed organizzative adeguate, efficaci e proporzionate allo scopo di garantire la sicurezza dei trattamenti, tenuto conto dei co-

sti in relazione a: stato dell'arte, natura dei dati, oggetto, contesto e finalità del trattamento, nonché dei rischi aventi probabilità e gravità differenti per i diritti e le libertà fondamentali delle persone fisiche (cd. "*privacy by design*");

- in particolare, attraverso l'adozione di siffatte misure, il Titolare tratta i dati in modo adeguato e pertinente (principio di minimizzazione) a quanto necessario rispetto ad ogni finalità del trattamento stesso (cd. "*privacy by default*");
- alla luce di quanto precede, il Titolare garantisce che il trattamento è effettuato in modo sicuro perché, fin dalla fase di progettazione dello stesso, adotta le relative misure ("*privacy by design*") e successivamente, per impostazione predefinita, tratta solo i dati indispensabili (minimizzazione) per ogni specifica finalità del trattamento ("*privacy by default*"),
- l'individuazione di un Responsabile della protezione dei dati (Data Protection Officer, in seguito, DPO) che, tra le altre funzioni, supporti il Titolare e i Dirigenti e vigili sulla corretta osservanza del GDPR all'interno dell'organizzazione del Titolare;

Richiamato, inoltre:

- l'articolo 37, paragrafo 1, lettera a) del succitato GDPR, che prevede l'obbligo per il Titolare di nominare il DPO quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;

Dato atto che:

- la Civica Amministrazione ha provveduto alla nomina del DPO attraverso ordinanza del Sindaco n. 163 del 18 maggio 2018, i cui contenuti si intendono integralmente richiamati;
- con successiva ordinanza del Sindaco n. 81 del 17 marzo 2020, in oggi in vigore, con la quale si è proceduto a prorogare l'incarico conferito al DPO per il Comune di Genova, a decorrere dal 13/03/2020, confermando, tra gli altri, il compito di provvedere alla tenuta, al mantenimento e all'aggiornamento del Registro del trattamento dei dati dell'Ente, nonchè disponendo che i compiti del DPO attengono all'insieme dei trattamenti effettuati dal Comune di Genova e stabilendo, infine, di mettere a disposizione del DPO le risorse umane e finanziarie necessarie al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate, anche attraverso la costituzione di un Gruppo di lavoro composto da dipendenti dell'Ente, già formati in materia di privacy;

Dato atto, inoltre, che:

- il Direttore della Direzione Sistemi Informativi ha predisposto il Registro delle attività di trattamento con determinazione dirigenziale n. 20 del 24 aprile 2018, i cui contenuti si intendono integralmente richiamati;
- il DPO ha integrato la procedura di gestione dei data breach, già approvata con la Comunicazione n. 6 del 24 luglio 2018, prot.n. 257199, mediante comunicazione n. 19 in data 22 ottobre 2019, prot.n. 367452;

Considerato che:

- il GDPR, oltre a indurre nel Titolare una sostanziale revisione delle *privacy policies*, dovuta principalmente all'applicazione del principio di responsabilizzazione, innova il lessico, in parte, i ruoli e le connesse responsabilità all'interno dell'organizzazione del Titolare e innesta all'interno della struttura organizzativa nuove responsabilità sulla protezione dei dati senza creare ulteriori figure, ritenendo che il dato personale, per il suo valore economico so-

ciale ed organizzativo, debba essere valutato come una risorsa assegnata alla responsabilità dell'azione dirigenziale, alla stregua di quelle umane e finanziarie;

Considerato inoltre che:

- a seguito dell'entrata in vigore del nuovo sistema normativo, comunitario e nazionale, di protezione delle persone fisiche con riguardo al trattamento dei dati personali, come sopra delineato, nonché avuto riguardo all'esigenza di garantire una sempre maggiore efficacia e efficienza dell'organizzazione interna, l'Amministrazione intende adeguare le proprie disposizioni in materia;

Valutato, pertanto, opportuno:

- in primo luogo, approvare il nuovo "REGOLAMENTO IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI" costituito dall'allegato A), quale parte integrante e sostanziale del presente provvedimento, con cui si dettano le disposizioni normative necessarie per l'adeguamento della struttura organizzativa del Comune di Genova alla disciplina nazionale e comunitaria in materia di protezione dei dati personali;
- in secondo luogo, apportare una breve modifica alla lettera b), comma 2 dell'articolo 23 del "Regolamento sull'ordinamento degli uffici e dei servizi", approvato con D.G.C n. 1121 del 16/07/1998, aggiornato al 08/04/2021, allo scopo di conformare il contenuto di detta lettera al sistema di cui sopra;

Dato atto, in particolare, che:

1. la citata disposizione, che si intende modificare, attualmente prevede che "*la funzione di "responsabile del trattamento dei dati personali" ai sensi e per gli effetti della normativa in materia, relativamente alle banche dati degli ambiti di competenza, individuando all'interno delle rispettive strutture gli "incaricati del trattamento" ed impartendo loro istruzioni scritte;*"

- le modifiche, riportate nel testo a fronte di cui all'allegato B), parte integrante e sostanziale del presente provvedimento, sono le seguenti:

  "*la funzione di "Designato al trattamento " - ai sensi e per gli effetti dell'art. 5 del Regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati - relativamente alle banche dati degli ambiti di competenza, individuando le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la sua diretta autorità, nel rispetto delle misure di sicurezza previste e delle istruzioni impartite*;"

Rilevata, per le medesime motivazioni sopra esposte e per l'effetto, l'opportunità di abrogare le seguenti disposizioni, che devono intendersi superate dal nuovo assetto normativo in materia di protezione dei dati personali:

1) il "Capo V - Norme sul trattamento dei dati personali" del vigente "Regolamento sul procedimento amministrativo e diritto di accesso", approvato con D.C.C. n. 39 del 26/07/2016, integrata con D.C.C. n. 55 del 22/11/2016, prevedendo fin d'ora che con separato provvedimento verranno adeguati i rinvii interni del medesimo regolamento alla disciplina sulla protezione dei dati personali;
2) il "Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20, comma 2, e 21, comma 2, D.Lgs. 30 giugno 2003, n. 196", con le relative schede allega-

te, adottato con D.C.C. n. 123 del 20/12/2005 e integrato con D.C.C n. 46 del 17/06/2008;

Valutato che:

detto sistema trova la propria positiva ricaduta in un'ottica di qualità dei servizi civici, anzitutto nei confronti di cittadini e imprese, destinatari dei servizi, e con l'obiettivo di contribuire a produrre un tangibile miglioramento della performance delle strutture dell'Amministrazione comunale;

Dato atto, infine, che:

- il presente provvedimento non comporta oneri riflessi diretti o indiretti sulla situazione economico-finanziaria sul patrimonio dell'Ente e, pertanto, non necessita del parere di regolarità contabile;
- il presente provvedimento sarà inviato, ai sensi dell'articolo 6, comma 3, dello Statuto comunale e a cura del DPO per il Comune di Genova, a tutti i Municipi per l'acquisizione del parere di competenza, parere da esprimersi entro il termine di venti giorni;
- ai sensi dell'articolo 6, comma 5, dello Statuto comunale, il testo del "REGOLAMENTO IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI", a seguito dell'esecutività del presente provvedimento, sarà pubblicato per quindici giorni all'Albo pretorio on line ed entrerà in vigore nel quindicesimo giorno successivo a quello della pubblicazione

Richiamato l'allegato parere in ordine alla regolarità tecnica del presente provvedimento, espresso dal DPO per il Comune di Genova, competente in materia;

Acquisito il visto di conformità del Segretario Generale, ai sensi dell'art. 97, comma 2 del D.Lgs. 18.8.2000, n. 267 (Testo Unico Enti Locali);

La GIUNTA
PROPONE
al Consiglio Comunale

1) di approvare il REGOLAMENTO IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI", individuato nel documento "Allegato A", parte integrante e sostanziale del presente provvedimento;

2) di modificare la lettera b), comma 2 dell'articolo 23 del vigente "Regolamento sull'ordinamento degli uffici e dei servizi", come espressamente indicato nel documento "Allegato B", parte integrante e sostanziale del presente provvedimento;

3) di abrogare il "Capo V - Norme sul trattamento dei dati personali" del vigente "Regolamento sul procedimento amministrativo e diritto di accesso", prevedendo fin d'ora che con separato provvedimento verranno adeguati i rinvii interni del medesimo regolamento alla disciplina sulla protezione dei dati personali;

4) di abrogare il “Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20, comma 2, e 21, comma 2, D.Lgs. 30 giugno 2003, n. 196”, con le relative schede allegate;
5) di dare atto che il presente provvedimento è stato redatto nel rispetto della normativa sulla protezione dei dati personali.

COMUNE DI GENOVA

CODICE UFFICIO: 980 0 0 1	**Proposta di Deliberazione N. 2021-DL-319 DEL 21/07/2021**

OGGETTO: Approvazione del "REGOLAMENTO IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI"

ELENCO ALLEGATI PARTE INTEGRANTE
allegato A regolamento protezione dati personali
allegato B testo a fronte art.23 regolamento uffici e servizi
allegato C relazione illustrativa al regolamento protezione dati

Il Dirigente
[Dott.ssa Luisa Gallo]

Documento Firmato Digitalmente

Allegato A)

COMUNE DI GENOVA

REGOLAMENTO
in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati

Approvato con deliberazione del Consiglio Comunale

In vigore dal

A cura del DPO (Data Protection Officer)

COMUNE DI GENOVA

Indice

Articolo 1
Oggetto e finalità del trattamento

1. La Civica Amministrazione tutela le persone fisiche con riguardo al trattamento dei dati personali e favorisce la libera circolazione degli stessi, conformando tutti i trattamenti ai principi del Regolamento Generale (UE) 2016/679 del Parlamento e del Consiglio dell'Unione Europea del 27 aprile 2016 (di seguito indicato con l'acronimo GDPR) e alla normativa nazionale di cui al Codice Privacy, approvato con D.LGS 30 giugno 2003, n. 196, come successivamente modificato dal D.LGS 10 agosto 2018, n. 101, che si intendono integralmente richiamati, per quanto non espressamente disciplinato dal presente Regolamento.
2. I dati sono trattati nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.
3. La Civica Amministrazione informa la propria azione alla suddetta normativa, in modo da garantire, ed essere in grado di dimostrare, che il trattamento è effettuato nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, e responsabilizzazione (accountability).
4. I trattamenti di dati personali svolti per il raggiungimento di compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita la Civica Amministrazione non necessitano del consenso dell'interessato, fatti salvi i casi previsti dalla legge, e rinvengono la propria base giuridica nell'art. 6 del GDPR.

Articolo 2
Ambito di applicazione

1. Le disposizioni contenute nel presente Regolamento si applicano a tutti i trattamenti di dati personali effettuati dalla Civica Amministrazione nello svolgimento delle proprie funzioni istituzionali e per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri.
2. Nel caso di trasferimento di dati personali verso un paese terzo, anche extra Unione Europea, o un'organizzazione internazionale, la Civica Amministrazione è responsabile del rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal GDPR.

Articolo 3
Titolare del trattamento

1. Il Titolare del trattamento, di seguito, Titolare, è la Civica Amministrazione, alla quale competono le decisioni in ordine alla finalità e ai mezzi del trattamento di dati personali, raccolti negli archivi digitali o cartacei all'interno delle strutture del Comune. La Civica Amministrazione, ai fini previsti dal GDPR, è rappresentata dal Sindaco *pro tempore*.
2. Il Sindaco nomina il Responsabile per la protezione dei dati (in seguito, DPO) per il Comune di Genova, ai sensi dell'art. 37 del GDPR, e secondo quanto specificato dal successivo articolo 7.
3. Il Titolare effettua il trattamento dei dati personali in modo conforme al GDPR, mettendo in atto misure tecniche e organizzative adeguate, efficaci e proporzionate allo scopo di garantire la sicurezza dei trattamenti, e agevola l'esercizio dei diritti con le modalità stabilite dal successivo articolo 4.
4. Gli interventi necessari per l'attuazione delle misure di cui al comma 3 sono considerati nell'ambito della programmazione operativa di cui al Documento Unico di Programmazione (DUP), al Piano Esecutivo di Gestione (PEG) e al bilancio, previa apposita analisi della

situazione in essere, tenuto conto dei costi che comporta il trattamento in relazione a: stato dell'arte, natura dei dati, oggetto, contesto e finalità del trattamento, nonché dei rischi aventi probabilità e gravità differenti per i diritti e le libertà delle persone fisiche.

5. Nell'effettuare tale analisi sono altresì considerate le positive ricadute del trattamento di dati personali in un'ottica di qualità dei servizi civici, anzitutto nei confronti di cittadini e imprese, destinatari dei servizi, e con l'obiettivo di contribuire a produrre un tangibile miglioramento della performance delle strutture dell'Ente.
6. Ove la Civica Amministrazione determini finalità e mezzi di un trattamento di dati personali congiuntamente ad altro soggetto, pubblico o privato, tale soggetto diviene contitolare del trattamento.
7. Qualora la Civica Amministrazione sia nominata Responsabile del trattamento, il Dirigente sottoscrive il relativo atto, provvedendo al rispetto delle istruzioni ricevute e alle previsioni del presente Regolamento.

Articolo 4
Esercizio dei diritti

1. Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del GDPR.
2. Se ritiene che il trattamento dei dati personali non sia conforme alle disposizioni vigenti ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti di cui al comma 1 non perviene nei tempi indicati o non è soddisfacente, l'interessato può rivolgersi all'Autorità Giudiziaria o all'Autorità di controllo (Garante per la protezione dei dati personali), in quest'ultimo caso mediante un reclamo ai sensi dell'art. 77 del GDPR.
3. L'istanza può essere riferita a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali, comunque trattati, ed è presentata alla Civica Amministrazione, senza formalità (es. posta elettronica, lettera raccomandata, etc.), fatte salve le limitazioni di cui agli artt. 2-*undecies* e 2-*duodeci*s del D.LGS 196/2003 e le altre limitazioni previste dalla legge.
4. L'istanza scritta è indirizzata al Titolare, tramite il DPO, o al Dirigente della struttura dove sono trattati i dati. Qualora il trattamento coinvolga più strutture, il Dirigente ricevente l'istanza ne dà comunicazione agli altri Dirigenti che detengono i dati personali dell'interessato.
5. Se il trattamento è effettuato da soggetti terzi per conto della Civica Amministrazione, sull'istanza è competente a rispondere il Dirigente che ha provveduto alla nomina del fornitore del servizio.
6. Il riscontro all'istanza presentata viene fornito, senza ingiustificato ritardo, entro 30 giorni dalla data di ricezione della stessa, anche nei casi di diniego.
7. Se le operazioni necessarie per il riscontro sono complesse o vi è una particolare e comprovata difficoltà, il termine dei 30 giorni può essere esteso fino a 2 mesi, non ulteriormente prorogabili. Di tale proroga viene data informazione all'interessato entro 20 giorni dalla ricezione dell'istanza.
8. L'interessato esercita i propri diritti attraverso opportune modalità gratuite e celeri. Il rilascio di documenti digitali e di copie digitali di documenti analogici è gratuito.
9. Solo nel caso in cui le istanze siano manifestamente infondate, eccessive o di carattere ripetitivo, può essere addebitabile un contributo spese ragionevole, il cui importo è fissato dall'Amministrazione, oppure il Dirigente può rifiutare di soddisfare la richiesta, dimostrandone il carattere manifestamente infondato, eccessivo o ripetitivo.

Articolo 5
Designati al trattamento

1. Il Sindaco, in qualità di legale rappresentante della Civica Amministrazione, Titolare del trattamento ai sensi dell'art. 4, par. 1, n. 7 del GDPR, e sotto la propria responsabilità, designa al trattamento i Dirigenti preposti alle strutture in cui si articola l'organizzazione comunale, delegando loro specifici compiti e funzioni in ordine alle finalità e ai mezzi connessi al trattamento di dati personali, funzionali ai compiti di ciascuna articolazione organizzativa.
2. Il Designato al trattamento garantisce, in relazione ai predetti compiti e funzioni, adeguata conoscenza specialistica; l'inosservanza delle direttive del Titolare può dare luogo a responsabilità disciplinare.
3. Il Designato al trattamento sovrintende, relativamente alle banche dati degli ambiti di competenza, a tutte le attività stabilite dalla legge ed esercita tutti i compiti e le funzioni allo stesso affidati dal Titolare, indicati specificamente nell'atto di delega, e concorre a realizzare il modello organizzativo privacy e, in particolare:

a) rende le informazioni sul trattamento dei dati personali previste dagli artt. 13 e 14 del GDPR, prima della raccolta dei dati, agevolando l'esercizio dei diritti dell'interessato;

b) per i trattamenti che hanno come base giuridica il consenso, adotta le misure organizzative atte a garantire la conservazione della copia del consenso acquisito;

c) predispone e aggiorna i Registri di cui al successivo articolo 12;

d) mette in atto misure tecniche ed organizzative adeguate, efficaci e proporzionate allo scopo di garantire la sicurezza del trattamento ai sensi del successivo articolo 10 e11;

e) riesamina ed aggiorna le misure di sicurezza relative alle banche dati digitali, d'intesa con il Responsabile della Transizione Digitale, sentito il Direttore preposto alla sicurezza dei sistemi informativi, con il supporto del DPO;

f) interloquisce e collabora con il DPO allo scopo di attuare prescrizioni e raccomandazioni emerse in sede di audit interni. Predispone inoltre, sempre in accordo con il DPO, un calendario di audit da svolgere congiuntamente, nei confronti dei Responsabili del trattamento e dei loro eventuali Sub-Responsabili del trattamento che trattano dati personali per conto della Civica Amministrazione, compresi audit a campione ovvero a rotazione;

g) individua, contrattualizza e nomina i Responsabili del trattamento;

h) relativamente alle banche dati degli ambiti di competenza, individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la sua diretta autorità, nel rispetto delle misure di sicurezza previste e delle istruzioni impartite. L'atto di incarico degli autorizzati al trattamento deve disciplinare:
   - la materia trattata, la durata, la natura e la finalità di trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie di interessati;
   - gli obblighi e i diritti del Titolare del trattamento;
   - le misure di sicurezza;
   - le istruzioni per il corretto trattamento.

i) effettua con le modalità di cui al successivo articolo 14, in accordo con il DPO, per la parte di competenza, prima di procedere al trattamento, la valutazione d'impatto sulla protezione dei dati nei casi in cui essa è obbligatoria o comunque opportuna;

j) svolge, con il supporto del DPO e con l'assistenza del Gruppo data breach, l'attività preliminare nei casi di presunto incidente di sicurezza di cui venga a conoscenza, secondo la *procedura di gestione dei data breach* di cui al successivo articolo 13.

Articolo 6
Responsabile del trattamento

1. Il Dirigente designato può avvalersi di soggetti esterni che svolgono per conto della Civica Amministrazione servizi o attività che implicano il trattamento di dati personali. Detti soggetti sono scelti in virtù dei requisiti di esperienza, capacità e affidabilità, in relazione alle peculiarità della materia di che trattasi.
2. Il Dirigente individua, contrattualizza e nomina i Responsabili del trattamento ai sensi dell'art. 28 del GDPR, avendo cura di specificare, fin dalla fase di scelta del contraente, le caratteristiche professionali e organizzative che essi devono possedere, in relazione alle peculiarità del servizio o del lavoro affidato;
3. Il Responsabile del trattamento - solo se autorizzato preventivamente per iscritto dal Dirigente - può avvalersi di soggetti terzi, cosiddetti Sub-Responsabili, e comunque nel rispetto degli obblighi contrattuali che lo legano al Titolare.
4. Il Dirigente, per mitigare i rischi derivanti dal trattamento, mette in atto opportuni strumenti che gli consentono di monitorare le attività affidate in outsourcing e trasmette periodicamente le risultanze all'Ufficio del DPO.
5. Le nomine dei Responsabili del trattamento sono annotate nel Registro delle attività di trattamento, ai sensi dell'art. 30 del GDPR e come meglio specificato dal successivo articolo 12, commi da 1 a 4, tenuto presso ciascuna Direzione del Comune di Genova.

Articolo 7
Responsabile della protezione dei dati (DPO)

1. Il Sindaco designa il Responsabile della protezione dei dati, in inglese, Data Protection Officer, nella figura unica di un dipendente di ruolo del Comune ovvero in un soggetto esterno scelto con procedura di evidenza pubblica.
2. L'individuazione del DPO avviene in funzione delle qualità professionali e di esperienza, delle conoscenze specialistiche della normativa e delle prassi di gestione dei dati personali.
3. Il nominativo del DPO, che svolge tutti i compiti previsti dal GDPR, è pubblicato e comunicato all'Autorità di controllo, con la quale coopera e funge da punto di contatto con essa, raccogliendo e comunicando tutte le informazioni relative al trattamento dei dati personali con particolare riferimento alle violazioni di dati personali e alla consultazione preventiva.
4. Il DPO opera in posizione di totale autonomia nello svolgimento dei compiti e delle funzioni ad esso attribuiti.
5. Il DPO, ferma restando l'indipendenza nello svolgimento dei compiti suoi propri, riferisce direttamente al Titolare e ai Designati al trattamento, e viene costantemente informato e coinvolto in tutte le decisioni riguardanti il trattamento dei dati personali.
6. Per le finalità del comma 5 sono organizzati periodici incontri con il Responsabile della transizione digitale e con il Responsabile della trasparenza e anticorruzione.
7. La figura del DPO è incompatibile con chi determina le finalità e i mezzi del trattamento, in particolare con il Responsabile della transizione digitale e con il Responsabile della trasparenza e anticorruzione.

Articolo 8
Ufficio del DPO

1. E' istituito l'Ufficio del DPO, come unità organizzativa di base, con competenze specialistiche e trasversali a tutte le strutture dell'Ente. L'ufficio funge da segreteria e supporto al DPO da cui dipende funzionalmente.

2. Il Titolare assegna all'ufficio adeguate risorse umane, finanziarie e strumentali per svolgere i propri compiti e garantisce l'accesso alle informazioni necessarie a fornire adeguato supporto alle Direzioni, anche predisponendo l'opportuna modulistica.
3. All'ufficio sono assegnati specifici obiettivi di PEG da conseguire durante l'esercizio finanziario e sono attribuite le seguenti competenze:

a) punto di riferimento multidisciplinare a supporto del Titolare e dei suoi Designati;

b) cura l'esercizio dei diritti di cui all'articolo 4;

c) cura le interlocuzioni con l'Autorità di controllo (Garante);

d) integra il Gruppo data breach con compiti di coordinamento e controllo degli adempimenti previsti dalla *procedura di gestione dei data breach*;

e) coadiuva il DPO nella redazione del piano annuale degli interventi finalizzati all'adeguamento al modello organizzativo privacy;

f) collabora con il DPO nella redazione del piano dei bisogni formativi dei Dirigenti e dei dipendenti in materia di privacy, concordando gli interventi con la Scuola di Amministrazione del Comune di Genova;

g) supporta il DPO nella redazione della Relazione annuale al Titolare;

h) accede ai Registri di cui all'articolo 12, tenuti sotto la responsabilità dei Dirigenti, che si avvalgono del Gruppo dei Referenti Privacy per il loro popolamento e aggiornamento;

i) supporta i Dirigenti nelle attività di audit, con particolare riguardo agli affidamenti in outsourcing.

Articolo 9
Gruppo dei Referenti Privacy

1. E' istituito il Gruppo dei Referenti Privacy, costituito da dipendenti dell'Ente, individuati dai rispettivi Dirigenti, quali autorizzati al trattamento dei dati personali, per le seguenti attività:

a) partecipare alle sessioni informative, formative e di sensibilizzazione in materia di protezione dei dati personali;

b) non diffondere dati, informazioni, notizie di cui si ha avuto conoscenza per ragioni di servizio;

c) coadiuvare il Dirigente nelle richieste di esercizio dei diritti dell'articolo 4;

d) segnalare tempestivamente anomalie, perdita, furto di dati personali, informando il proprio Dirigente, con le modalità previste dalla *procedura di gestione dei data breach*.

2. In assenza di formale designazione, coloro che trattano dati personali nell'ambito del rapporto con la Civica Amministrazione sono comunque ritenuti autorizzati al trattamento dei dati personali e sono obbligati a osservare quanto previsto dal presente Regolamento.
3. L'accesso ai dati personali da parte degli autorizzati al trattamento è soddisfatto in via diretta e senza ulteriori formalità nella misura necessaria al perseguimento dell'interesse istituzionale, ferma restando la responsabilità personale derivante dall'utilizzo improprio dei dati e dalla violazione delle istruzioni ricevute.
4. L'elenco dei Referenti Privacy è approvato con determinazione del DPO, revisionato periodicamente ed aggiornato ad ogni variazione. La figura del Referente Privacy può essere condivisa tra più strutture, qualora ciò sia compatibile con la complessità e l'omogeneità dei trattamenti presenti.
5. Il Gruppo dei Referenti Privacy si riunisce periodicamente, sotto il coordinamento del DPO, per esaminare problematiche di tipo trasversale e concordare le modalità organizzative più efficaci ed efficienti in materia di protezione dei dati personali.

Articolo 10
Amministratori di sistema

1. I Dirigenti, in relazione ai trattamenti di loro competenza, provvedono a designare gli Amministratori di sistema tra i propri dipendenti o, se necessario, tra soggetti esterni.
2. Qualora la designazione degli Amministratori di sistema riguardi soggetti esterni al Comune di Genova, la competenza è del Dirigente che ha provveduto all'affidamento del contratto in base al quale viene sviluppato o gestito il software, viene strutturata o gestita la banca dati informatica o, comunque, viene effettuato il trattamento.
3. Ciascuna Direzione predispone un elenco degli Amministratori di sistema che condivide con i Sistemi Informativi dell'Ente.

Articolo 11
Sicurezza del trattamento

1. Il Dirigente mette in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, secondo una pianificazione concordata con il DPO.
2. Il Dirigente riesamina e aggiorna in modo periodico le misure, d'intesa con il Responsabile della transizione Digitale, sentito il Direttore preposto alla sicurezza dei sistemi informativi e con il supporto del DPO. Tali aggiornamenti sono pubblicati sulla rete Intranet e illustrati nelle sessioni formative.
3. La Civica Amministrazione, considerato il rischio connesso al trasporto di dati personali su supporto rimovibile (es. computer portatili, smartphone, chiavette USB, disco fisso portatile, copie cartacee, etc.), soprattutto con riguardo a categorie particolari di dati, grandi volumi di dati e informazioni che comportano particolari rischi per l'interessato nei casi di perdita, furto di dati personali, ne disincentiva l'utilizzo.
4. Salvo le attività che per loro natura devono essere effettuate al di fuori dell'ambiente di lavoro, i dati personali possono essere trasportati all'esterno del perimetro aziendale in circostanza eccezionali e sotto la diretta responsabilità del personale autorizzato. In particolare, il personale autorizzato è tenuto a:

   a) ove possibile, fare uso di accesso remoto tramite login e password alle informazioni in possesso alla Civica Amministrazione;

   b) trasportare all'esterno del perimetro aziendale solo la quantità minima di dati personali trattati per ragioni di servizio;

   c) assicurarsi che i dispositivi mobili e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali, fuori dall'ambiente di lavoro, siano dotati di sistemi di crittografia e i documenti cartacei siano contenuti all'interno di plichi chiusi.
5. Qualunque perdita, furto di dati personali deve essere tempestivamente segnalato e trattato, con le modalità previste dalla *procedura di gestione dei data breach*.

Articolo 12
Registri

1. Il Registro delle attività di trattamento è il registro dell'Ente che contiene le informazioni relative alle attività svolte da ciascuna direzione. Detto registro è predisposto e aggiornato costantemente dal Dirigente, relativamente alle banche dati degli ambiti di competenza, avvalendosi del Gruppo dei Referenti Privacy relativamente al popolamento dei trattamenti e dell'anagrafica dei responsabili esterni del trattamento (fornitori).

2. Per la parte relativa all'anagrafica dei fornitori devono essere indicati, in particolare: gli estremi del contratto di affidamento, sua decorrenza e scadenza, la determinazione dirigenziale di affidamento, il provvedimento di nomina del fornitore in veste di Responsabile del trattamento, l'eventuale autorizzazione ad avvalersi di soggetti Sub-Responsabili del trattamento, la data di eventuale non rinnovo del contratto di fornitura del servizio con indicazione di avvenuta cancellazione ovvero di restituzione dei dati personali e di eventuali copie.
3. Il Gruppo dei Referenti Privacy inoltra all'Ufficio del DPO sintetici report semestrali di aggiornamento anagrafico dei Responsabili esterni e degli eventuali Sub-Responsabili del trattamento, evidenziando la data di scadenza e di rinnovo, ove previsto, delle nomine.
4. Nel registro possono essere annotate anche le attività di trattamento ritenute rilevanti, quali ad esempio le valutazioni d'impatto sulla protezione dei dati (DPIA) già effettuate o ancora in fieri nonché i casi di specifici trattamenti di dati sensibili e giudiziari.
5. Il Registro dei data breach è il registro dell'Ente ove il Dirigente provvede ad annotare le violazioni di dati personali che si sono verificate all'interno della Direzione ma anche i data breach comunicati dai fornitori esterni, ai quali ha affidato servizi che implicano il trattamento di dati personali.
6. Entrambi i registri sono a messi a disposizione dell'Autorità di controllo.

Articolo 13
Gruppo data breach

1. E' istituito il Gruppo data breach formato da Referenti Privacy e da un funzionario dell'Ufficio del DPO che agiscono in stretta collaborazione con i Sistemi Informativi, secondo la *procedura di gestione dei data breach*, approvata dal Titolare, con comunicazione del DPO e pubblicata nella Intranet, spazio privacy.
2. Il Gruppo ha compiti di gestione operativa degli adempimenti previsti al verificarsi di una emergenza data breach con l'obbligo di reperibilità e continuità.
3. Alle attività del Gruppo può essere eventualmente invitato a partecipare un delegato del Responsabile del trattamento o del Sub-Responsabile del trattamento dove si è verificato l'incidente di sicurezza.
1. Al Gruppo è garantita una corretta informazione e una specifica formazione.

Articolo 14
Valutazione d'impatto sulla protezione dei dati (DPIA)

1. Il Dirigente ha l'obbligo di effettuare - prima dell'inizio del trattamento - e con il supporto del DPO, una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment), laddove il trattamento stesso possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità.
2. Qualora il Dirigente non concordi con le indicazioni rese nel parere del DPO, è necessario che documenti le motivazioni per cui non ha ritenuto di conformarsi al parere e, in tal caso, la decisione è rimessa al Segretario Generale.
3. Qualora il DPO esprima parere non favorevole perché la DPIA ha indicato che il trattamento presenterebbe un rischio elevato e si tratti di compiti di particolare rilevanza per le attività istituzionali dell'Amministrazione il Dirigente - prima di rivolgersi al Garante - rimette la decisione al Segretario Generale.
4. Nel caso in cui sia previsto che il trattamento venga eseguito in tutto o in parte da un Responsabile del trattamento o da un suo Sub-Responsabile del trattamento il soggetto esterno assiste il

Dirigente nell'esecuzione della DPIA, sempre con il supporto del DPO, tenendo conto della natura del trattamento e delle informazioni disponibili.

Articolo 15
Disposizioni transitorie e finali

1. Con l'entrata in vigore delle disposizioni di cui al presente Regolamento **è abrogato il *"Capo V – Norme sul trattamento dei dati personali***" del **Regolamento sul procedimento amministrativo e diritto di accesso**.
2. Con l'entrata in vigore delle disposizioni di cui al presente Regolamento **è modificata la *lett. b), c. 2 dell'art. 23*** del "**Regolamento sull'ordinamento degli uffici e dei servizi**" al posto delle parole: "*la funzione di "responsabile del trattamento dei dati personali" ai sensi e per gli effetti della normativa in materia, relativamente alle banche dati degli ambiti di competenza, individuando all'interno delle rispettive strutture gli "incaricati del trattamento" ed impartendo loro istruzioni scritte;*" è inserito il seguente testo: "**la funzione di "Designato al trattamento" - ai sensi e per gli effetti dell'art. 5 del Regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati - relativamente alle banche dati degli ambiti di competenza, individuando le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la sua diretta autorità, nel rispetto delle misure di sicurezza previste e delle istruzioni impartite;**".
3. Con l'entrata in vigore delle disposizioni di cui al presente Regolamento **è abrogato l'intero** "**Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20, comma 2, e 21, comma 2, D.Lgs. 30 giugno 2003, n. 196**" **con le relative schede allegate.**
4. Le disposizioni di cui al presente Regolamento entrano in vigore nel quindicesimo giorno successivo a quello della loro pubblicazione, ai sensi dell'articolo 6, comma 5, dello Statuto del Comune di Genova e sono inoltre pubblicate sul portale dell'Amministrazione nell'apposito spazio dei Regolamenti comunali.

Allegato B)

REGOLAMENTO SULL'ORDINAMENTO DEGLI UFFICI E DEI SERVIZI

PARTE I
L'ORGANIZZAZIONE

TESTO ATTUALE	TESTO MODIFICATO
TITOLO III - FUNZIONI DI DIREZIONE DELL'ENTE	**TITOLO III - FUNZIONI DI DIREZIONE DELL'ENTE**
Art. 23 – Dirigenti	Art. 23 – Dirigenti
1. Ai dirigenti, compresi i direttori, sono affidate tutte le funzioni previste dalla legge e dallo Statuto; essi in relazione al rispettivo ambito di competenza, adottano tutti gli atti di gestione amministrativa, finanziaria, tecnica ed organizzativa per dare attuazione alle direttive, ai programmi ed alle disposizioni dell'Amministrazione e per conseguire gli obiettivi indicati nel piano esecutivo di gestione. Nello svolgimento delle suddette attività i dirigenti rispondono ai direttori di riferimento.	1. Ai dirigenti, compresi i direttori, sono affidate tutte le funzioni previste dalla legge e dallo Statuto; essi in relazione al rispettivo ambito di competenza, adottano tutti gli atti di gestione amministrativa, finanziaria, tecnica ed organizzativa per dare attuazione alle direttive, ai programmi ed alle disposizioni dell'Amministrazione e per conseguire gli obiettivi indicati nel piano esecutivo di gestione. Nello svolgimento delle suddette attività i dirigenti rispondono ai direttori di riferimento.
2. I dirigenti cui sia affidata la direzione di strutture organizzative esercitano: a) la funzione di dirigente prevista dalla normativa in tema di salute e sicurezza nei luoghi di lavoro attuando le direttive del Direttore che esercita le funzioni di datore di lavoro, organizzando l'attività lavorativa e vigilando su di essa; b) la funzione di "responsabile del trattamento dei dati personali" ai sensi e per gli effetti della normativa in materia, relativamente alle banche dati degli ambiti di competenza, individuando all'interno delle rispettive strutture gli "incaricati del trattamento" ed impartendo loro istruzioni scritte; c) la funzione di responsabile dell'Archivio Corrente e dell'Archivio di Deposito nei quali è conservata la documentazione prodotta o ricevuta dagli uffici facenti parte della struttura organizzativa cui sovrintendono.	2. I dirigenti cui sia affidata la direzione di strutture organizzative esercitano: a) la funzione di dirigente prevista dalla normativa in tema di salute e sicurezza nei luoghi di lavoro attuando le direttive del Direttore che esercita le funzioni di datore di lavoro, organizzando l'attività lavorativa e vigilando su di essa; b) **la funzione di "Designato al trattamento " - ai sensi e per gli effetti dell'art. 5 del Regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati - relativamente alle banche dati degli ambiti di competenza, individuando le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la sua diretta autorità, nel rispetto delle misure di sicurezza previste e delle istruzioni impartite;** c) la funzione di responsabile dell'Archivio Corrente e dell'Archivio di Deposito nei quali è conservata la documentazione prodotta o ricevuta dagli uffici facenti parte della struttura organizzativa cui sovrintendono.

3. Ferme restando le disposizioni contenute negli articoli 12 comma 3, art. 25 comma 2 bis, laddove non in contrasto con la presente disposizione, i Direttori a cui afferiscono le strutture in materia di mercati, scuole, servizi civici e cimiteriali, servizi sociali, musei, biblioteche, teatri e impianti sportivi esercitano la funzione di Datore di Lavoro ai sensi delle disposizioni contenute all'interno del D. Lg.s. n. 81/08 s.m.i. in tema di salute e sicurezza nei luoghi di lavoro.	3. Ferme restando le disposizioni contenute negli articoli 12 comma 3, art. 25 comma 2 bis, laddove non in contrasto con la presente disposizione, i Direttori a cui afferiscono le strutture in materia di mercati, scuole, servizi civici e cimiteriali, servizi sociali, musei, biblioteche, teatri e impianti sportivi esercitano la funzione di Datore di Lavoro ai sensi delle disposizioni contenute all'interno del D. Lg.s. n. 81/08 s.m.i. in tema di salute e sicurezza nei luoghi di lavoro.
4. Al fine di garantire la regolare esecuzione degli interventi di manutenzione ordinaria secondo le modalità previste dalla normativa vigente devono essere assegnate ai Datori di Lavoro adeguate risorse finanziarie.	4. Al fine di garantire la regolare esecuzione degli interventi di manutenzione ordinaria secondo le modalità previste dalla normativa vigente devono essere assegnate ai Datori di Lavoro adeguate risorse finanziarie.
5.Relativamente all'esecuzione degli interventi di manutenzione straordinaria, Il Datore di Lavoro ne risponde nei limiti stabiliti dall'art. 18, comma 3, del D.Lgs. n. 81 del 2008.	5.Relativamente all'esecuzione degli interventi di manutenzione straordinaria, Il Datore di Lavoro ne risponde nei limiti stabiliti dall'art. 18, comma 3, del D.Lgs. n. 81 del 2008.
6. Qualora la funzione di Datore di lavoro sia esercitata relativamente a strutture in cui insistono parti comuni o condivise facenti capo a più Datori di lavoro, sarà datore di lavoro di tali spazi comuni il soggetto apicale cui sono assegnati il maggior numero di dipendenti e, in caso di parità degli stessi, a cui sono assegnati maggiori spazi (criterio della prevalenza).	6. Qualora la funzione di Datore di lavoro sia esercitata relativamente a strutture in cui insistono parti comuni o condivise facenti capo a più Datori di lavoro, sarà datore di lavoro di tali spazi comuni il soggetto apicale cui sono assegnati il maggior numero di dipendenti e, in caso di parità degli stessi, a cui sono assegnati maggiori spazi (criterio della prevalenza).
7. Sono denominati Direttori, ai fini del presente Regolamento, i dirigenti preposti alle Direzioni.	7. Sono denominati Direttori, ai fini del presente Regolamento, i dirigenti preposti alle Direzioni.
8. I Direttori collaborano con i Coordinatori delle Aree, con il Direttore Generale e con gli organi di governo all'elaborazione delle strategie, mediante l'elaborazione di studi, piani di fattibilità, progetti e valutazioni di alternative; inoltre, coordinano l'azione dei dirigenti presenti all'interno della Direzione, con idonei strumenti atti a verificare e valutare i risultati della loro attività.	8. I Direttori collaborano con i Coordinatori delle Aree, con il Direttore Generale e con gli organi di governo all'elaborazione delle strategie, mediante l'elaborazione di studi, piani di fattibilità, progetti e valutazioni di alternative; inoltre, coordinano l'azione dei dirigenti presenti all'interno della Direzione, con idonei strumenti atti a verificare e valutare i risultati della loro attività.
9. In caso di assenza e/o impedimento temporanei del direttore preposto ad una delle strutture organizzative dell'Ente, un dirigente delle strutture che ad esso riferiscono ne svolge le funzioni, sulla base delle indicazioni ricevute dal direttore stesso.	9. In caso di assenza e/o impedimento temporanei del direttore preposto ad una delle strutture organizzative dell'Ente, un dirigente delle strutture che ad esso riferiscono ne svolge le funzioni, sulla base delle indicazioni ricevute dal direttore stesso.
10. In caso di assenza e/o impedimento temporanei di un dirigente, le relative funzioni sono espletate dal direttore di riferimento o dal dirigente che svolge le funzioni del direttore ai sensi di quanto sopra disposto.	10. In caso di assenza e/o impedimento temporanei di un dirigente, le relative funzioni sono espletate dal direttore di riferimento o dal dirigente che svolge le funzioni del direttore ai sensi di quanto sopra disposto.

11. Nel caso in cui non sia applicabile quanto sopra, le funzioni sono svolte dal Direttore Generale ovvero da altro Direttore preventivamente individuato. 12. E' fatta salva, in ogni caso, la facoltà del Sindaco di attribuire le funzioni del direttore/dirigente assente e/o impedito con un incarico ad interim. 13. In caso di inadempienza o di constatata inerzia da parte di un Dirigente rispetto a singoli provvedimenti, il Direttore Generale procede a diffida scritta, fissando un termine per l'adempimento. In caso di ulteriore inerzia, il Direttore Generale propone al Sindaco i provvedimenti da adottare compresa la revoca dell'incarico, previo contraddittorio, integrando l'inadempimento e l'inerzia gravi violazioni ai doveri di ufficio. 14. Nel caso in cui non siano assegnati alla struttura altri Dirigenti oltre al Direttore, il Coordinatore dell'Area svolge le funzioni di quest'ultimo, fatte salve diverse disposizioni del Direttore Generale.	11. Nel caso in cui non sia applicabile quanto sopra, le funzioni sono svolte dal Direttore Generale ovvero da altro Direttore preventivamente individuato. 12. E' fatta salva, in ogni caso, la facoltà del Sindaco di attribuire le funzioni del direttore/dirigente assente e/o impedito con un incarico ad interim. 13. In caso di inadempienza o di constatata inerzia da parte di un Dirigente rispetto a singoli provvedimenti, il Direttore Generale procede a diffida scritta, fissando un termine per l'adempimento. In caso di ulteriore inerzia, il Direttore Generale propone al Sindaco i provvedimenti da adottare compresa la revoca dell'incarico, previo contraddittorio, integrando l'inadempimento e l'inerzia gravi violazioni ai doveri di ufficio. 14. Nel caso in cui non siano assegnati alla struttura altri Dirigenti oltre al Direttore, il Coordinatore dell'Area svolge le funzioni di quest'ultimo, fatte salve diverse disposizioni del Direttore Generale.

REGOLAMENTO
in materia di protezione delle persone fisiche
con riguardo al trattamento dei dati personali
nonché alla circolazione di tali dati

Relazione illustrativa

Premessa

Il Comune di Genova ha disciplinato la materia della protezione dei dati personali (comunemente detta "privacy") nel *Capo V* "*Norme sul trattamento dei dati personali*" del "Regolamento in materia di procedimento amministrativo, diritto di accesso, disciplina delle dichiarazioni sostitutive e trattamento dei dati personali" approvato con deliberazione del Consiglio Comunale n. 39 del 26/07/2016, integrato con deliberazione del Consiglio Comunale n. 55 del 22/11/2016.

Si propone ora una completa revisione di tale disciplina al fine di renderla più aderente alle previsioni del Regolamento generale (UE) del Parlamento e del Consiglio dell'Unione europea 2016/679, altrimenti noto con l'acronimo GDPR, che ha uniformato le legislazioni dei Paesi europei in tale materia.

Il legislatore europeo ha inteso adeguare la disciplina al mutato contesto politico, economico e sociale che rileva per tre principali motivi: anzitutto, il rapido sviluppo delle nuove tecnologie, nemmeno immaginabile negli anni che chiudevano il secolo scorso (es. *social networks*, *cloud computing*, *Internet of things*, *data analytics* e *big data*, *modelli di intelligenza artificiale*, *blockchain*, *etc.*), che hanno reso obsolete le previgenti disposizioni; in secondo luogo, l'incremento del numero di Stati Membri, che ha determinato l'esigenza di definire una strategia funzionale alla creazione di una economia dei dati, come fattore determinante per promuovere un mercato unico digitale.

Da quanto precede emerge un valore intrinseco del dato personale e la conseguente necessità per l'Amministrazione di predisporre adeguate misure di sicurezza, atte a tutelare il dato stesso perché ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano nel rispetto della dignità umana, dei diritti e delle libertà fondamentali, garantendone, al contempo, la libera circolazione, quale fattore indispensabile per la crescita economica e la produzione di nuovi beni e servizi.

Il GDPR è informato al principio di responsabilizzazione (cd. *di accountability* - artt. 5 e 24) ovvero alla necessità che l'Amministrazione comunale, titolare del trattamento (d'ora in avanti, Titolare), si doti del modello organizzativo ritenuto più idoneo, in relazione alle proprie esigenze e peculiarità dei processi organizzativi, allo scopo di garantire la gestione sicura del dato.

Le presenti disposizioni, delle quali si propone l'adozione, hanno lo scopo quindi di dotare l'Ente del modello organizzativo privacy adeguato al proprio assetto organizzativo generale e di dimostrare la concreta attuazione delle misure finalizzate ad assicurare la *compliance* (rispetto, aderenza, conformità) delle scelte operate dal Comune di Genova al GDPR.

In altre parole, la Civica Amministrazione, in qualità di Titolare, determina le finalità e i mezzi del trattamento nonché le misure di sicurezza e quindi ha maggiore discrezionalità nel decidere come le strutture comunali debbano conformarsi alle disposizioni del GDPR, ma ha anche l'onere di comprovare l'effettiva adeguatezza delle misure adottate al fine di attuare in modo efficace i principi di protezione dei dati e tutelare i diritti degli interessati.

In tal senso il principio di *accountability* va letto sotto un duplice profilo: esso non è soltanto il principio che ispira l'adeguamento/l'adempimento dell'Amministrazione alla disciplina in materia di protezione dei dati, ma è anche il punto di partenza per dimostrare la *compliance* delle scelte organizzative operate dal Titolare a tale impianto normativo.

In conclusione, rispetto al Codice privacy, il GDPR impone l'abbandono del mero adempimento burocratico a favore di un approccio basato sul rischio (cd. di r*isk-based*) *fin dalla progettazione* di misure organizzative adeguate, efficaci e proporzionate allo scopo di garantire la sicurezza dei trattamenti e prevenire possibili danni dovuti a incidenti di sicurezza o data breach.

L'adozione di questo approccio implica la necessità per l'Amministrazione di programmare interventi finalizzati a mettere in atto dette misure, attraverso formazione, informazione e comunicazione al fine di sviluppare una maggiore consapevolezza nei dipendenti rispetto ai rischi del trattamento e far comprendere che il dato va considerato e trattato come una risorsa dotata di elevato valore sociale ed economico per migliorare i servizi civici al cittadino e alle imprese.

DESCRIZIONE DELL'ARTICOLATO

La presente proposta di Regolamento si compone di 15 articoli di cui di seguito s'illustra più dettagliatamente il contenuto:

Articolo 1 - Oggetto e finalità del trattamento

L'oggetto delle presenti disposizioni è l'adeguamento della struttura organizzativa dell'Ente alla disciplina comunitaria e nazionale in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione degli stessi.

L'articolo, dopo aver richiamato i principi generali del trattamento dell'articolo 1 del Codice Privacy, elenca i principi comunitari applicabili al trattamento sanciti all'articolo 5 del GDPR, tra i quali la responsabilizzazione o *accountability* del Titolare in base alla quale il medesimo è tenuto ad adottare comportamenti proattivi che assicurino, ed essere in grado di dimostrare, che il trattamento è effettuato nel rispetto del citato articolo 5.

Tali comportamenti si riassumono in un approccio organizzativo e tecnologico in relazione alle proprie esigenze e peculiarità, allo scopo di assicurare la gestione sicura del dato, quali la concreta adozione di *ragionevoli misure tecniche ed organizzative* adeguate efficaci e proporzionate allo scopo di garantire la sicurezza del trattamento, mitigando il rischio di furto, accesso non autorizzato, distruzione di informazioni personali, e il *rafforzamento dell'esercizio dei diritti* dell'interessato in relazione ai propri dati personali.

La protezione dei dati sulla base dell'articolo 5 in combinato disposto con l'articolo 25 del GDPR deve iniziare fin dalla progettazione del trattamento (*privacy by design*) e deve essere per impostazione predefinita (*privacy by default*). La matrice comune di questi due precetti risiede nel principio di "*minimizzazione dei dati*" di cui all'articolo 5, paragrafo 1, lettera c) del GDPR, in quanto il trattamento deve riguardare soltanto i dati necessari alle specifiche finalità previste.

Nell'ultimo comma sono esplicitate le finalità del trattamento di dati comuni (es. nome e cognome, codice fiscale, etc.) dentro il quadro di legge dettato dalla lettera e), paragrafo 1 dell'articolo 6 del GDPR.

Articolo 2 - Ambito di applicazione

Nel comma 1 si afferma che il Regolamento si applica a tutti i trattamenti effettuati dall'Amministrazione, non solo ai *dati comuni*, ma anche le altre categorie di dati personali: *dati sensibili* e *dati giudiziari*, i cui principi sono contenuti rispettivamente negli articoli 9 e 10 del GDPR.

Il comma 2 contiene un richiamo al CAPO V Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali del GDPR e significa che l'Amministrazione è tenuta ad adottare comportamenti che assicurino, ed essere in grado di dimostrare, che il trattamento è effettuato nel rispetto dei principi di cui all'articolo 5 del GDPR.

Articolo 3 - Titolare del trattamento

Il comma 1 definisce le caratteristiche soggettive e le responsabilità della Civica Amministrazione, rappresentata dal Sindaco *pro tempore* che, ai sensi dell'articolo 4, paragrafo 1, numero 7 del GDPR, in qualità di Titolare assume le decisioni circa le finalità, le modalità del trattamento e l'adozione di adeguate misure di sicurezza di cui all'articolo 32 del GDPR.

Nel comma 2 viene esplicitato che il Sindaco nomina il DPO ai sensi dell'articolo 37, paragrafo 1, lettera a) del GDPR e si assicura che svolga effettivamente i compiti attribuiti dall'articolo 39 del GDPR.

Il comma 4 è molto importante perché stabilisce che le misure adeguate alla sicurezza del trattamento debbano essere considerate nell'ambito degli strumenti di programmazione e di attuazione degli obbiettivi programmatici dell'Ente. Tale comma ricalca i contenuti del paragrafo 2 dell'articolo 38 del GDPR nella parte in cui è previsto che il Titolare nel sostenere il DPO nell'esecuzione dei propri compiti, gli fornisca le risorse necessarie per assolvere a tali compiti.

Nel comma 6 è prevista l'ipotesi di contitolarità di cui all'articolo 26 del GDPR ossia qualora il trattamento venga effettuato congiuntamente da due o più titolari. In tale situazione la norma prevede che i soggetti si accordino per definire reciproche responsabilità e rispettive funzioni al fine di garantire il rispetto delle prerogative degli interessati.

Nell'ultimo comma è previsto il caso nel quale la Civica Amministrazione assuma il ruolo soggettivo di responsabile del trattamento di cui all'articolo 28 del GDPR e quindi si trovi a trattare i dati personali per conto di un titolare che determina finalità e mezzi del trattamento.

Articolo 4 - Esercizio dei diritti

L'intero sistema di protezione delle persone fisiche con riguardo al trattamento dei dati personali, è concepito per incrementare il livello di sicurezza di gestione delle informazioni personali, come illustrato in premessa,

Pertanto, prima dell'inizio del trattamento, il Titolare deve fornire una informativa specifica, differenziata a seconda che i dati vengano raccolti presso l'interessato con i contenuti degli articoli 13 e 14 del GDPR; rispetto al Codice Privacy, sono state estese le informazioni che il Titolare deve fornire qualora all'interessato nell'esercizio dei diritti previsti agli articoli da 15 a 22 del GDPR.

L'articolo descrive l'intera procedura gratuita e celere per l'esercizio dei diritti.

Articolo 5 - Designati al trattamento

Viene introdotta nell'Amministrazione comunale la figura del "Designato al trattamento" che subentra alla vecchia figura del Responsabile (interno) del trattamento, ex articolo 29 del Codice Privacy, non più prevista dal GDPR.

L'articolo opera una qualificazione del ruolo dei Dirigenti presso i quali si svolgono i singoli trattamenti, in relazione alle banche dati degli ambiti di competenza, ciò al fine di creare un forte legame tra gestione delle risorse umane e finanziarie e gestione del dato, tutti elementi necessari che concorrono al raggiungimento degli obiettivi prefissati.

Articolo 6 - Responsabile del trattamento

Il Responsabile del trattamento (di seguito, Responsabile) è definito dall'articolo 4, paragrafo 1, numero 8 del GDPR come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali "per conto" del titolare del trattamento.

Tale figura non deve essere confusa con quella avente la medesima denominazione prevista dal previgente regime (responsabile del trattamento, articolo 29, Codice Privacy), né può essere ridotta a mero referente esterno del Titolare. L'articolo 28 del GDPR costruisce il rapporto tra Titolare e Responsabile come un incarico che prevede degli obblighi reciproci: essenzialmente il primo deve fornire delle istruzioni documentate al secondo, il quale deve dimostrare di adottarle.

Per tale motivo si può sostenere che la relazione tra Titolare e Responsabile rappresenti il punto in cui si realizza in modo più compiuto uno dei pilastri del GDPR, ossia il principio di "responsabilizzazione": tutti i soggetti destinatari delle disposizioni del GDPR non devono soltanto adeguarsi ad esso, ma porsi nelle condizioni di poter dimostrare di averlo fatto, qualora ciò venga richiesto dall'Autorità di controllo (Garante privacy).

L'articolo è costruito sulla responsabilizzazione del Dirigente, delegato da Sindaco a compiere specifici compiti e funzioni in ordine alle finalità e ai mezzi connessi al trattamento di dati personali, funzionali ai compiti di ciascuna articolazione organizzativa.

Il Responsabile viene individuato per il possesso di requisiti di esperienza, capacità e affidabilità ed è previsto che possa avvalersi di soggetti terzi, cosiddetti Sub-responsabili del trattamento solo se preventivamente autorizzato per iscritto e comunque nel rispetto degli obblighi contrattuali che lo legano al Titolare.

Articolo 7 - Responsabile della protezione dei dati (DPO)

Poiché l'Amministrazione rientra nella fattispecie prevista dall'articolo 37, paragrafo 1, lettera a) del GDPR ha provveduto a nominare il DPO con ordinanza del Sindaco.

La figura del DPO è descritta nello standard tecnico UNI 11697:2017: Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza. Si tratta, in estrema sintesi, di una figura con elevate competenze specialistiche.

È importante sottolineare che il DPO non è un semplice consulente, bensì un soggetto a cui sono attribuiti molteplici compiti direttamente dalla legge e, più precisamente, dall'articolo 39 del GDPR; tra questi compiti vi sono, tra gli altri, la sorveglianza e la cooperazione con il Garante nell'accertamento di eventuali trattamenti illeciti.

Ferma restando l'indipendenza nello svolgimento dei compiti, il DPO riferisce direttamente al Titolare e ai Designati e viene costantemente informato e coinvolto in tutte le decisioni riguardanti il trattamento dei dati personali. Il DPO ha rapporti, per via delle attività svolte, con il Responsabile della transizione digitale e con il Responsabile della trasparenza e anticorruzione.

Articolo 8 - Ufficio del DPO

Per l'ottimale svolgimento dei compiti, il DPO necessita di un Ufficio, al quale sono assegnati specifici obiettivi di PEG da conseguire durante l'esercizio finanziario e gli sono attribuite competenze volte all'attuazione della *compliance* dell'Amministrazione al GDPR.

L'ufficio funziona da segreteria e supporto specialistico al DPO da cui dipende funzionalmente, per questo motivo l'ufficio non può essere collocato all'interno di una direzione che ha compiti di amministrazione diretta ma piuttosto collocato all'interno di una struttura di Staff.

Articolo 9 - Gruppo dei Referenti Privacy

Pur non prevedendo espressamente la figura dell'incaricato del trattamento di cui all'abrogato articolo 30 del Codice Privacy, il GDPR non ne esclude la presenza, in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" di cui all'articolo 4, paragrafo 1, numero 10 del GDPR. Inoltre, l'articolo 2-quaterdecies del Codice Privacy ha introdotto la figura della persona autorizzata a svolgere compiti e funzioni connessi al trattamento di dati personali che opera sotto la diretta responsabilità del Dirigente.

Pertanto, ai sensi delle norme citate il Dirigente dovrà autorizzare i propri dipendenti ad effettuare le attività di trattamento in relazione alle banche dati degli ambiti di competenza. Il Gruppo dei Referenti Privacy è costituito dunque da dipendenti dell'Amministrazione, individuate dai rispettivi Dirigenti, quali autorizzati al trattamento per il disbrigo degli adempimenti in materia di protezione dei dati personali e per agevolare l'esercizio dei diritti dell'interessato.

L’elenco dei referenti è approvato con determinazione dirigenziale del DPO.

Articolo 10 - Amministratori di sistema

L’articolo è stato costruito sul provvedimento del Garante [doc. web n. 1626595], raggiungibile al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499 relativo alla figura dell’amministratore di sistema (AdS) del 2008, aggiornato nel 2009; i provvedimenti citati sono da considerarsi tutt’ora applicabili perché compatibili con le disposizioni del GDPR.

La designazione di AdS è individuale e reca l’elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi, con l’elenco delle funzioni attribuite, devono essere riportati in un documento interno, aggiornato e disponibile nel caso di accertamenti da parte del Garante privacy.

Qualora l’attività dell’AdS riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, il Titolare è tenuto a rendere nota o conoscibile l’identità degli AdS nell’ambito delle proprie organizzazioni, in relazione ai diversi servizi informatici cui questi sono preposti, ciò avvalendosi dell’informativa resa agli interessati ai sensi dell’articolo 13 del GDPR.

Articolo 11 - Sicurezza del trattamento

L’approccio basato sulla valutazione del rischio (cd. risk based) di cui all’articolo 32 del GDPR esige che il Titolare garantisca l’intera filiera del trattamento, ossia *fin dalla progettazione* (privacy by design), adottando ragionevoli misure di sicurezza contro rischi, quali la perdita o l’accesso non autorizzato, la distruzione, l’utilizzo, la modifica o la divulgazione dei dati stessi e, successivamente, *per impostazione predefinita*, trattando solo i dati indispensabili (principio di minimizzazione dell’articolo 5, paragrafo 1, lettera c) del GDPR) per ogni specifica finalità del trattamento (privacy by default).

Articolo 12 – Registri

Il GDPR richiede una rigorosa formalizzazione delle modalità di effettuazione del trattamento, ossia richiede al Titolare e al Responsabile uno sforzo sotto il profilo dell’onere della prova circa la sussistenza dei requisiti che legittimano il trattamento.

Detta prova risulta soddisfatta con la predisposizione e l’aggiornamento del Registro dei trattamenti che, ai sensi dell’articolo 30 del GDPR, Titolare e Responsabile sono tenuti ad esibire all’Autorità di controllo (Garante privacy) su richiesta di quest’ultima.

Il Registro dei data breach è anch’esso un documento di prova, predisposto e aggiornato dal Dirigente, relativamente alle banche dati degli ambiti di trattamento, nel quale vengono annotate sia tutte le violazioni di dati all’interno della direzione sia quelle comunicate dai Responsabili ex articolo 28, GDPR e da eventuali Sub-responsabili.

Entrambi i registri sono a messi a disposizione dell’Autorità Garante.

Articolo 13 - Gruppo data breach

Il Gruppo data breach come figura normativa non è prevista, tuttavia se ne propone l’introduzione per la sua rilevanza operativa. Il Gruppo è composto da un certo numero di dipendenti dell’Amministrazione che agiscono a stretto contatto con il DPO e i Sistemi Informativi allo scopo di gestire dal punto di vista operativo gli adempimenti al verificarsi di una emergenza data breach e per questi motivi hanno l’obbligo di reperibilità e continuità.

Relativamente all’obbligo di notifica di una violazione di dati personali, l’articolo 33 del GDPR prevede che il Titolare, qualora subisca una violazione che metta in pericolo i dati personali che tratta, debba informarne senza ritardo il Garante privacy e, a certe condizioni, anche l’interessato (articolo 34, GDPR). La notifica va fatta entro il termine perentorio di 72 ore dal momento in cui si

ha avuto conoscenza, dettagliando l'incidente di sicurezza o l'attacco informatico subito e indicando le misure adottate per rimediare agli eventuali danni.

Articolo 14 - Valutazione d'impatto sulla protezione dei dati (DPIA)

La valutazione di impatto sulla protezione dei dati (DPIA dall'inglese *Data Protection Impact Assessment*) di cui all'articolo 35 del GDPR va considerato come un processo di monitoraggio costante, con il quale il Titolare documenta sia le analisi del rischio, effettuate in relazione ai più delicati trattamenti di dati personali, sia le soluzioni adottate per mitigare i rischi e limitare gli eventuali danni.

Proprio sulla base della DPIA, il Titolare, nel caso di sinistro, deve dimostrare che le misure predisposte erano comunque "adeguate" al trattamento - non solo necessarie e nemmeno idonee - e che, di conseguenza, "*l'evento dannoso non gli è in alcun modo imputabile*" ai sensi dell'articolo 82, paragrafo 3 del GDPR.

Articolo 15 - Disposizioni transitorie e finali

L'articolo contiene le disposizioni comunali non più compatibili con il GDPR.

Più precisamente, si propone di apportare una **modifica alla lettera b), comma 2 dell'articolo 23** del "Regolamento sull'ordinamento degli uffici e dei servizi", approvato con D.G.C n. 1121 del 16/07/1998, aggiornato al 08/04/2021, allo scopo di conformare detta lettera alla disciplina in materia di protezione dei dati personali.

In particolare, **il contenuto della citata lettera b)** è il seguente: "*la funzione di "responsabile del trattamento dei dati personali" ai sensi e per gli effetti della normativa in materia, relativamente alle banche dati degli ambiti di competenza, individuando all'interno delle rispettive strutture gli "incaricati del trattamento" ed impartendo loro istruzioni scritte.*"

Il nuovo testo sarà il seguente: "*la funzione di "Designato al trattamento " - ai sensi e per gli effetti dell'art. 5 del Regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati - relativamente alle banche dati degli ambiti di competenza, individuando le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la sua diretta autorità, nel rispetto delle misure di sicurezza previste e delle istruzioni impartite*;"

Rilevata l'opportunità **di abrogare** per i due regolamenti comunali, come di seguito indicato, in quanto risultano superati dal nuovo sistema di protezione dei dati personali e, più precisamente:

1. **il "Capo V - Norme sul trattamento dei dati personali"** del "Regolamento sul procedimento amministrativo e diritto di accesso", approvato con D.C.C. n. 39 del 26/07/2016, integrata con D.C.C. n. 55 del 22/11/2016 e di prevedere che con separato provvedimento verranno adeguati i rinvii interni del medesimo regolamento alla disciplina sulla protezione dei dati personali;
2. **il "Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20, comma 2, e 21, comma 2, D.Lgs. 30 giugno 2003, n. 196", con le relative schede allegate,** adottato con D.C.C. n. 123 del 20/12/2005 e integrato con D.C.C n. 46 del 17/06/2008.

L'articolo dispone infine in ordine all'entrata in vigore delle disposizioni proposte e la pubblicazione sul portale dell'Amministrazione.

COMUNE DI GENOVA

E' PARTE INTEGRANTE DELLA PROPOSTA DI DELIBERAZIONE N. 2021-DL-319 DEL 21/07/2021 AD OGGETTO: Approvazione del "REGOLAMENTO IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI"

PARERE TECNICO (Art 49 c. 1 D.Lgs. 267/2000)
Si esprime parere favorevole in ordine alla regolarità tecnica del presente provvedimento da parte della Dott.ssa Luisa Gallo in veste di Responsabile protezione dati (DPO) per il Comune di Genova, competente in materia.

21/07/2021

Il Dirigente Responsabile DPO
[Dott.ssa Luisa Gallo]

Documento Firmato Digitalmente