Comune di Padova

REGOLAMENTO COMUNALE PER L'ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679 E DEL D.Lgs. 196/2003 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Approvato con deliberazione di Consiglio comunale n. 61 del 11/09/2023 in vigore dal 11/10/2023

Indice dei contenuti

Art. 1 - Oggetto

1. Il presente Regolamento ha per oggetto misure di procedura e regole di dettaglio ai fini della corretta ed effettiva attuazione nel Comune di Padova del Regolamento dell'Unione Europea relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, adottato dal Parlamento Europeo ed il Consiglio dell'Unione Europea in data 27 aprile 2016 n. 679 (*General Data Protection Regulation* - Regolamento Generale Protezione Dati, di seguito indicato con "GDPR"), nonché delle norme attuative vigenti, con particolare riferimento al D.lgs. 196/2003 e successive modificazioni ed integrazioni.

Art. 2 - Definizioni

Ai fini del presente Regolamento, si intende per:

a) **Titolare del trattamento:** il Comune di Padova, in quanto soggetto che unitariamente determina finalità e mezzi del trattamento di dati personali.
b) **Soggetto Designato:** il/la Dirigente Capo Settore espressamente designato/a ai sensi dell'art 2-*quaterdecies* D.lgs. 196/2003, al/alla quale sono attribuiti specifici compiti e funzioni relativi al trattamento dei dati personali.
c) **Soggetti Autorizzati:** personale opportunamente istruito e nominato ai sensi dell'art. 29 GDPR che ha accesso ai dati personali ed opera sotto l'autorità dei Soggetti Designati.
d) **Responsabile del trattamento:** soggetto pubblico o privato, esterno rispetto all'organizzazione dell'Ente, che tratta dati personali per conto di quest'ultimo ai sensi dell'art. 28 GDPR.
e) **Sub-Responsabile del trattamento:** soggetto incaricato dal Responsabile del trattamento ai sensi dell'art. 28 par. 4 GDPR per l'esecuzione di specifiche attività di trattamento svolte per conto del Titolare del trattamento.
f) **Contitolare:** qualunque soggetto, pubblico o privato, con il quale il Titolare del trattamento intrattiene un rapporto di contitolarità ai sensi dell'art. 26 GDPR riferito ad uno specifico trattamento il cui fine ed i mezzi sono congiuntamente determinati.
g) **Responsabile per la protezione dati (DPO):** il/la dipendente della struttura organizzativa del Titolare, il professionista privato o impresa esterna, incaricato ai sensi dell'art. 37 GDPR.
h) **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (*interessato/a*) attraverso, ad esempio, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale, ai sensi dell'art. 4 par. 1 GDPR.
i) **Registro delle attività di trattamento del Titolare del trattamento:** insieme dei Registri dei trattamenti di Settore tenuti in forma telematica da ciascun/ciascuna Dirigente Capo Settore secondo le rispettive competenze e contenenti gli elementi richiesti all'art. 30 GDPR.
j) **Valutazione d'impatto sulla protezione dei dati (DPIA):** procedura finalizzata a descrivere un trattamento comportante un rischio elevato, valutarne necessità e

proporzionalità, e facilitare la gestione e la prevenzione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, ai fini di dimostrarne la conformità rispetto alle previsioni normative.

k) **Violazione di dati personali / Data breach:** qualsiasi violazione di sicurezza accertata o in corso di accertamento che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati.

l) **Garante:** Garante per la Protezione dei Dati Personali istituito dalla Legge 31 dicembre 1996 n. 675, quale Autorità amministrativa pubblica di controllo indipendente.

Art. 3 - Titolare del trattamento

1. Il Comune di Padova, rappresentato ai fini previsti dal GDPR dal/dalla Sindaco/a *pro tempore*, è il Titolare del trattamento dei dati personali (di seguito indicato con "Titolare") e determina le finalità ed i mezzi del trattamento stesso (art. 4 par. 7 GDPR). I dati oggetto di trattamento possono essere raccolti sia su supporti cartacei che digitali, con o senza l'ausilio di processi automatizzati, in esecuzione di attività istituzionali o delegate ed esclusivamente per le finalità specificate dal GDPR.

2. Il Titolare è competente, ai sensi dell'art 5 GDPR, per il rispetto dei principi fondamentali del trattamento dei dati personali: ovvero liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

3. Ai sensi degli artt.. 25 e 32 del GDPR il Titolare, fin dalla fase di progettazione, dispone e mette in atto le necessarie misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio e che il trattamento dei dati personali sia effettuato in conformità al GDPR e alla normativa allo stato vigente in materia di protezione dei dati personali.

4. In ogni caso il Titolare mette in atto misure per garantire che i dati siano trattati per impostazione predefinita, ossia stabilendo sin dall'inizio quali sono i dati personali strettamente necessari a ciascuna finalità di trattamento, in osservanza dei summenzionati principi di minimizzazione e di limitazione della conservazione. Gli interventi necessari per l'attuazione di tali misure sono considerati nell'ambito degli strumenti di programmazione, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

5. Il Titolare fornisce agli interessati, ovverosia qualunque persona fisica identificata o identificabile i cui dati personali sono trattati dal Titolare o da altro soggetto che tratta i dati per conto del medesimo:

a) tutte le informazioni di cui all'art. 13 GDPR, qualora i dati personali siano raccolti direttamente presso gli interessati;
b) tutte le informazioni di cui all'art. 14 GDPR, qualora i dati personali non siano stati raccolti direttamente presso gli interessati.

6. Ai sensi dell'art. 35 GDPR e dell'art. 11 del presente Regolamento, il Titolare è tenuto ad effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito

indicata con "DPIA", *Data Protection Impact Assessment*) qualora un determinato tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

7. Il Titolare agevola l'esercizio dei diritti degli interessati stabiliti dagli artt. 15-22 GDPR, nonché di tutte le comunicazioni e le informazioni occorrenti per l'esercizio di tale diritto.

8. Il Titolare può avvalersi, per il trattamento dei dati, di soggetti esterni nominati quali Responsabili del trattamento ai sensi dell'art. 7 del presente Regolamento.

9. Il Titolare può ricorrere alla stipula di accordi di contitolarità ai sensi dell'art. 8 del presente Regolamento.

10. Il Titolare attribuisce specifici compiti e funzioni, ai sensi dell'art. 2-*quaterdecies* D.lgs. 196/2003, ai/alle Dirigenti Capo Settore espressamente designati/e ed in possesso di adeguate competenze. I soggetti così individuati (di seguito "Designati" o "Soggetti Designati") sono preposti al trattamento dei dati contenuti nelle banche dati esistenti delle articolazioni dei Settori di loro competenza. Ad essi il Titolare del trattamento può conferire ulteriori compiti e funzioni in relazione alle attività svolte dal Settore, quali la nomina di Responsabili del trattamento ai sensi dell'art. 28 GDPR, la costituzione di Accordi di Contitolarità ai sensi dell'art. 26 GDPR, nonché qualsiasi altro compito o funzione espressamente indicato nell'atto di designazione.

11. Il Titolare si impegna a favorire l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione in materia di protezione dei dati di cui al capo IV, sezione V, del GDPR, per contribuire alla corretta applicazione della normativa vigente e per dimostrare il concreto rispetto di essa da parte del Titolare e dei Soggetti Designati.

Art. 4 - Finalità del trattamento

1. Un trattamento può essere compiuto dal Titolare qualora il trattamento si dimostri lecito ai sensi di quanto disposto dal GDPR e, ove pertinente, dal D.lgs. 196/2003.

2. Il trattamento di *dati personali "comuni"* è considerato lecito nella misura in cui ricorre almeno una delle seguenti condizioni:

a) ai sensi dell'art. 6 par. 1 lett. b) GDPR: in esecuzione di un contratto di cui il Titolare è parte o all'esecuzione di misure precontrattuali su richiesta degli interessati;
b) ai sensi dell'art. 6 par. 1 lett. c) GDPR: per l'adempimento di un obbligo legale al quale è soggetto il Titolare;
c) ai sensi dell'art. 6 par. 1 lett. d) GDPR: per la salvaguardia degli interessi vitali degli interessati o di un'altra persona fisica;
d) ai sensi dell'art. 6 par. 1 lett. e) GDPR in combinato disposto con l'art. 2-*ter* D.lgs. 196/2003: in esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare. In particolare, rientrano in questo ambito i trattamenti compiuti per:
   i. l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;

ii. la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e statistica;
iii. l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale o regionale delegate al Comune in base alla vigente legislazione, ovvero per altri servizi in base a convenzione.

e) il trattamento è comunque sempre lecito ai sensi dell'art. 2-*ter* D.Lgs. 196/2003: in esecuzione di una norma di legge, di un regolamento o di un atto amministrativo generale.

3. Il trattamento di *categorie particolari di dati personali*, così come definite dall'art. 9 par. 1 GDPR, è considerato lecito:

a) ai sensi dell'art. 9 par. 2 lett. b) quando il trattamento è necessario in quanto effettuato in adempimento di obblighi in materia del diritto del lavoro, della sicurezza sociale e della protezione sociale;
b) ai sensi dell'art. 9 par. 2 lett. f) quando il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
c) ai sensi dell'art. 9 par. 2 lett. g) in combinato disposto con l'art. 2-*sexies* D.lgs. 196/2003, quando il trattamento è ritenuto necessario in quanto effettuato per motivi di interesse pubblico rilevante.
   L'interesse pubblico è considerato rilevante quando il trattamento è previsto dal diritto dell'Unione europea ovvero da disposizioni di legge dell'ordinamento interno o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili ed il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati. Si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti d'interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie indicate al comma 2 dell'articolo 2 sexies del D.Lgs 196/2003 , lettere da a) a dd).
d) ai sensi dell'art. 9 par. 2 lett. h) quando il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, o per la necessaria valutazione della capacità lavorativa del/della dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari;
e) ai sensi dell'art. 9 par. 2 lett. j) quando il trattamento è necessario a fini di archiviazione nel pubblico interesse sulla base del diritto dell'Unione europea o del diritto nazionale, che preveda garanzie adeguate per i diritti e le libertà degli interessati.

4. Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'art. 6 par. 1 GDPR deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione europea o degli Stati Membri che preveda garanzie appropriate per i diritti e le libertà degli interessati, in conformità con l'art. 10 GDPR. Ai sensi dell'art. 2-*octies* comma 5 D.lgs. 196/2003, al trattamento dei dati di cui al presente comma si applicano le medesime disposizioni previste dall'articolo 2-*sexies* D.lgs. 196/2003.

5. Per specifiche finalità diverse da quelle di cui ai precedenti punti, il trattamento è lecito purché gli interessati esprimano il consenso al trattamento in conformità con l'art. 6 par. 1 lett. a) GDPR, e, nel caso di trattamenti aventi ad oggetto categorie particolari di dati personali, ai sensi dell'art. 9

par. 2 lett. a) GDPR, purché tale consenso sia informato, libero, specifico e inequivocabile, ovverosia risponda ai requisiti di cui all'art. 7 GDPR.

6. È sempre necessario evidenziare agli interessati la base giuridica addotta a fondamento del trattamento, in virtù dei principi di liceità, correttezza e trasparenza.

Art. 5 - Soggetti Designati dal Titolare del trattamento

1. Ciascun/ciascuna Dirigente Capo Settore è designato/a ai sensi dell'art. 2-*quaterdecies* del D.lgs. 196/2003 con decreto del/della Sindaco/a quale "Soggetto Designato", preposto al trattamento di tutti i dati personali esistenti nel proprio Settore, secondo l'articolazione organizzativa di rispettiva competenza. Il decreto di designazione del/della Sindaco/a disciplina gli specifici compiti e funzioni connessi al trattamento dei dati personali attribuiti nonché la durata, la natura, la finalità, il tipo di dati personali e le categorie di interessati dei trattamenti assegnati in relazione al Settore di competenza.

2. Il Soggetto Designato deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 9 del presente Regolamento, adeguate a garantire che i trattamenti siano effettuati in conformità al GDPR.

3. Ciascun Soggetto Designato nomina quale "Soggetto Autorizzato" ai sensi dell'art. 29 GDPR chiunque agisca sotto la propria autorità e che abbia accesso a dati personali (dipendenti del Settore e tutti gli altri soggetti che collaborano a qualsiasi titolo, ivi compresi stagisti e volontari), garantendo che questi sia adeguatamente formato ed impegnato alla riservatezza. La nomina di Soggetto Autorizzato al trattamento dei dati personali deve essere disposta con atto scritto e deve necessariamente contenere:

a) istruzioni operative relative alla mansione specifica svolta, ivi comprese le modalità di trattamento dei dati personali, con riferimento ai trattamenti svolti con e senza l'ausilio di strumenti elettronici;
b) descrizione delle categorie di dati personali trattate e degli interessati;
c) durata, natura e finalità del trattamento;
d) obblighi in capo al Soggetto Autorizzato;
e) eventuali autorizzazioni specifiche relative all'utilizzo di strumenti di lavoro dai quali possa derivare un trattamento di dati personali.

4. Ciascun Soggetto Designato può avvalersi, qualora previsto dall'atto di designazione ed in ordine all'esercizio delle attività istituzionali, di soggetti esterni ai sensi dell'art. 7 del presente Regolamento, per far svolgere loro specifiche attività di trattamento.

5. Ciascun Soggetto Designato può costituire, qualora previsto dall'atto di designazione ed in ordine all'esercizio delle attività istituzionali, accordi di contitolarità ai sensi dell'art. 8 del presente Regolamento.

6. Ciascun Soggetto Designato provvede, per il proprio Settore di competenza, a tutti i compiti affidatigli dal Titolare ai sensi dell'art. 2-*quaterdecies* D.lgs. 196/2003 contenuti nel decreto di designazione. In particolare, provvede:

a) alla tenuta ed aggiornamento del proprio Registro di Settore relativo alle attività di trattamento svolte per conto del Titolare (c.d. Registro delle attività di trattamento, di cui all'art. 30 GDPR ed all'art. 10 del presente Regolamento);
b) all'adozione di idonee misure tecniche ed organizzative adeguate a garantire la sicurezza dei trattamenti ai sensi dell'art. 32 GDPR, nonché ad effettuare analisi dei rischi al fine di valutare preventivamente l'adeguatezza delle misure individuate;
c) alla redazione e/o revisione della DPIA di cui all'art. 11 del presente Regolamento, in relazione ai trattamenti del Settore di competenza, coordinandosi con gli ulteriori Uffici comunali coinvolti qualora il trattamento dei dati personali sia trasversale a più settori;
d) ad informare il Titolare ed a consultarsi tempestivamente con il Responsabile della Protezione dei Dati della venuta a conoscenza e/o dell'accertamento di casi di violazione dei dati personali relativi ai trattamenti del proprio Settore, nonché ad adottare le misure indicate dal GDPR in caso di violazione dei dati personali;
e) a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo, nonché contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da altro soggetto da questi incaricato.

7. Ulteriori ed eventuali figure, che non siano Dirigenti Capo Settore, possono altresì essere designate con decreto del Sindaco ai sensi dell'art. 2-*quaterdecies* del D.lgs. 196/2003, per motivate ragioni organizzative. Ad esse non si applicano le disposizioni specificatamente dirette ai "Soggetti Designati" di cui al presente Regolamento: la competenza, i compiti assegnati e le specifiche attribuzioni sono invece disciplinate esclusivamente dall'atto di designazione costituito dal decreto del Sindaco.

Art. 6 - Responsabile della protezione dei dati

1. Il Responsabile della protezione dei dati del Comune di Padova (in seguito indicato con "DPO", *Data Protection Officer*) è individuato con provvedimento dirigenziale del Settore in cui è incardinata l'Unità organizzativa specificatamente dedicata alla gestione della privacy (d'ora in poi denominata "Unità organizzativa privacy") di cui al successivo art. 15. Esso è scelto in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art. 39 GDPR. Il DPO può essere un/una dipendente del Titolare del trattamento, fatte salve le cause di incompatibilità di cui al comma 6 del presente articolo, oppure un soggetto esterno espressamente incaricato.

2. Il DPO è incaricato dei seguenti compiti:
a) dare informazioni e fornire consulenza al Titolare ed ai Soggetti Designati nonché ai/alle dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalla normativa relativa alla protezione dei dati. In tal senso il DPO può indicare al Titolare i settori funzionali ai quali riservare un audit in tema di protezione dei dati, verificando inoltre le attività di formazione interna per il personale che tratta dati personali;
b) sorvegliare l'osservanza del GDPR e della normativa relativa alla protezione dei dati, ferma restando la responsabilità del Titolare;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dai Soggetti Designati in materia di protezione dei dati personali;
d) fornire al Titolare, se richiesto, un parere in merito alla DPIA di cui all'art. 11 del presente Regolamento, in ordine a particolari procedimenti amministrativi che comportano trattamento di dati personali ed un rischio per i diritti e per le libertà delle persone fisiche, e sorvegliarne lo svolgimento;
e) cooperare con il Garante per la Protezione dei Dati Personali (in seguito indicato con "Garante") e fungere da punto di contatto tra il Titolare e detta Autorità per questioni connesse al trattamento dei dati, tramite lo strumento della consultazione preventiva di cui all'art. 36 GDPR ed effettuare, se del caso, consultazioni relativamente a ogni altra questione;
f) supportare il Titolare ed i Soggetti Designati nella tenuta dei Registri di trattamento di cui all'art. 10 del presente Regolamento;
g) fornire consulenza in ordine ad ulteriori attività, a condizione che il Titolare o il Soggetto Designato accertino che tali compiti e funzioni non diano adito ad un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

3. Il Titolare, i Soggetti Designati ed i Responsabili del trattamento assicurano che il DPO sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
a) sostengono il DPO nell'adempimento del proprio incarico, fornendogli le risorse necessarie per assolvere tali compiti, ivi compresa la possibilità di accedere ai trattamenti, affinché questo possa mantenere la propria conoscenza specialistica;
b) invitano il DPO a partecipare alle riunioni di coordinamento dei/delle Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
c) forniscono tempestivamente al DPO tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, affinché lo stesso sia posto nelle condizioni per fornire una consulenza idonea, scritta od orale;
d) prendono in considerazione e documentano il parere del DPO sulle decisioni che impattano sulla protezione dei dati, la cui presa in esame è obbligatoria ma non vincolante. Nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal DPO, è necessario motivare specificamente tale decisione;
e) consultano tempestivamente il DPO qualora si verifichi una violazione dei dati o un altro incidente di sicurezza.

4. Nello svolgimento dei compiti affidatigli, fermo restando l'obbligo al segreto od alla riservatezza, il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il DPO:
a) procede alla stesura di un report iniziale contenente una mappatura delle aree di attività e di organizzazione del Comune, evidenziandone il grado di conformità e di rischio nei termini di protezione dei dati, fornendo inoltre delle indicazioni per l'adozione di misure di miglioramento o correttive qualora dovesse rilevare situazioni di mancato od insufficiente adeguamento da parte del Titolare;

b) definisce un ordine di priorità nell'attività da svolgere - ovverosia un piano annuale di attività - incentrandola sulle aree che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed ai Soggetti Designati;

5. Il DPO dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

6. La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili gli incarichi di:

a) responsabile per la prevenzione della corruzione e per la trasparenza di cui alla legge 190/2012;
b) responsabile del trattamento nominato ai sensi dell'art. 28 GDPR;
c) qualunque incarico o funzione che comporti la determinazione di finalità o mezzi del trattamento.

7. Il Titolare e ciascun Soggetto Designato forniscono al DPO le risorse necessarie per assolvere i compiti attribuiti e per sorvegliare sui dati personali e sui trattamenti. In particolare è assicurato al DPO:

a) supporto attivo per lo svolgimento dei propri compiti, garantendo la collaborazione di tutti coloro che rivestono ruoli di responsabilità e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della gestione delle attività e dei servizi comunali, degli strumenti di programmazione e del Piano Performance;
b) supporto tramite la costituzione della Unità organizzativa privacy di cui al successivo art. 15, ed eventualmente, ove ritenuto opportuno, di un gruppo di lavoro apposito;
c) comunicazione ufficiale della nomina del DPO a tutto il personale effettuata tramite intranet aziendale, in modo da garantire che la sua presenza e le sue funzioni siano rese note all'interno dell'Ente;
d) accesso garantito ai settori funzionali dell'Ente, al fine di ottenere supporto, informazioni ed indicazioni essenziali.

8. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti. In particolare, non deve ricevere istruzioni in merito allo svolgimento delle proprie mansioni né circa l'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il DPO non può essere rimosso o penalizzato dal Titolare e dai Soggetti Designati per l'adempimento dei propri compiti.

9. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare ed ai Soggetti Designati. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Soggetto Designato direttamente coinvolto.

10. I nominativi ed i dati di contatto del Titolare e del DPO sono resi pubblici attraverso la sezione Amministrazione trasparente. Il Soggetto Designato presso cui è incardinata l'Unità organizzativa privacy trasmette tempestivamente la nomina del DPO al Garante.

Art. 7 - Responsabile del trattamento

1. Il Titolare del trattamento ovvero il Soggetto Designato, qualora previsto dall'atto di designazione e comunque entro i limiti di attività di trattamento dati attribuiti al proprio Settore, può ricorrere a soggetti esterni al fine di affidare a questi uno o più trattamenti di propria competenza. La nomina di Responsabile del trattamento ai sensi dell'art. 28 GDPR deve avvenire sotto forma di contratto scritto; tale nomina deve necessariamente contenere le seguenti informazioni, relative al trattamento esternalizzato:

a) oggetto e durata del trattamento;
b) natura e finalità del trattamento, ovverosia la puntuale descrizione delle operazioni eseguite nell'ambito di trattamento nonché gli obbiettivi che il trattamento desidera perseguire;
c) tipologia dei dati personali, comprensiva di una dettagliata elencazione dei dati personali oggetto di trattamento;
d) misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio poste in essere da parte del Responsabile del trattamento a protezione dei dati trattati;
e) categorie di interessati;
f) obblighi e diritti del Titolare del trattamento, ivi compreso: il diritto del Titolare di effettuare ispezioni ed attività di revisione; l'obbligo di collaborazione e di rigorosa osservanza delle disposizioni della normativa vigente da parte del Responsabile;
g) una procedura di gestione dei potenziali eventi di violazione dei dati personali che consenta al Titolare di adempiere tempestivamente agli obblighi imposti dalla normativa in merito alla segnalazione delle violazione medesima al Garante ed alla comunicazione della stessa agli interessati (artt. 33 e 34 GDPR)

2. Si procede di norma alla nomina di un Responsabile del trattamento nei casi di soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

3. Il Responsabile del trattamento potrà avvalersi, previa consultazione ed approvazione da parte del Titolare o del Soggetto Designato, di ulteriori soggetti da egli nominati (c.d. sub-responsabili) con apposito atto giuridico, che assumano i medesimi obblighi in materia di protezione dei dati personali contenuti nel proprio atto di nomina a Responsabile. Il Responsabile del trattamento conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei sub-responsabili.

4. L'individuazione delle responsabilità tra Titolare, Responsabile ed eventuali sub-responsabili, con riferimento al dovere di risarcimento di chiunque abbia subito un danno materiale o immateriale dalla violazione delle disposizioni vigenti in materia di dati personali, è disciplinata dall'art. 82 GDPR.

Art. 8 - Accordi di contitolarità

1. Il Titolare del trattamento ovvero il Soggetto Designato, qualora previsto dall'atto di designazione e comunque entro i limiti di attività di trattamento dati attribuiti al proprio Settore, può

ricorrere ad accordi di contitolarità di cui all'art. 26 GDPR, al fine di determinare congiuntamente con un altro Titolare o con più Titolari le finalità ed i mezzi di uno specifico trattamento.

2. L'accordo, stipulato in forma scritta, deve determinare le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con riguardo all'esercizio dei diritti degli interessati e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 GDPR. Dall'accordo deve inoltre chiaramente risultare la ripartizione delle attività tra i Titolari. Ciascun accordo di contitolarità deve necessariamente contenere:

a) oggetto e durata del trattamento;
b) natura e finalità del trattamento, come inteso nel precedente articolo;
c) tipologie di dati trattati, come inteso nel precedente articolo;
d) l'attuazione dei principi generali di protezione dati di cui all'art. 5 GDPR;
e) la base giuridica a fondamento del trattamento per ciascun Titolare;
f) le misure di sicurezza poste in essere da ciascun Titolare che garantiscano un livello di sicurezza adeguato al rischio;
g) una procedura di gestione tra i Titolari dei potenziali eventi di violazione dei dati personali, ivi compresa la notifica al Garante ed agli interessati (artt. 33 e 34 GDPR);
h) la disciplina relativa al ricorso ad un Responsabile del trattamento ai sensi dell'art. 28 GDPR;
i) l'organizzazione del contatto con gli interessati, ovverosia la ripartizione dei compiti in merito all'obbligo di somministrazione della informativa;

3. Se pertinente rispetto al trattamento oggetto di contitolarità, ovverosia in presenza dei requisiti di cui all'art. 11 del presente Regolamento, l'accordo deve prevedere anche la produzione di una DPIA ai sensi dell'art. 35 GDPR, il cui svolgimento può essere ripartito tra le parti.

4. L'accordo di contitolarità si applica esclusivamente al trattamento il cui fine e mezzi sono congiuntamente determinati dai Titolari. Qualunque trattamento diverso od addizionale rispetto a quelli specificati all'interno dell'accordo di cui sopra costituisce un trattamento ulteriore, per il quale è responsabile, in qualità di Titolare autonomo, il solo Titolare che lo ha messo in atto.

5. L'individuazione delle responsabilità tra Titolari in regime di contitolarità, con riferimento al dovere di risarcimento di chiunque abbia subito un danno materiale o immateriale dalla violazione delle disposizioni vigenti in materia di dati personali, è disciplinata dall'art. 82 GDPR.

Art. 9 - Sicurezza del trattamento

1. Il Titolare del trattamento ed i Soggetti Designati, in ordine a ciascun trattamento effettuato dall'Ente, mettono in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche, 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, assicurando la protezione dei dati fin dalla progettazione, ovvero per impostazione predefinita.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento di cui all'art. 32 GDPR comprendono, a titolo esemplificativo: pseudonimizzazione;

minimizzazione; cifratura dei dati personali; capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; 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.

3. Costituiscono misure tecniche ed organizzative, fatti salvi ulteriori provvedimenti e linee guida che dovessero integrare o modificare quelle qui sotto elencate a titolo esemplificativo e non esaustivo:

a) Linee guida EDPB 3/2019 sul trattamento di dati personali attraverso dispositivi video, versione 2.0 adottate il 29 gennaio 2020;
b) Linee guida EDPB 4/2019 sull'art. 25 GDPR - Protezione dei dati fin dalla progettazione e per impostazione predefinita, versione 2.0, adottate il 20 ottobre 2020;
c) Linee guida ICT: Circolare AgID del 18 aprile 2017, n. 2/2017 (*Pubblicato in Gazzetta Ufficiale Serie Generale n. 103 del 5 maggio 2017*);
d) Garante per la protezione dei dati personali: Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.lgs. 10 agosto 2018, n. 101 del 5 giugno 2019 (*Pubblicato in Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019*);
e) Garante per la protezione dei dati personali: Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati del 15 maggio 2014 (*Pubblicato in Gazzetta Ufficiale Serie Generale n. 134 del 12 giugno 2014);*
f) Garante per la protezione dei dati personali: Provvedimento in materia di videosorveglianza dell'8 aprile 2010 (*Pubblicato in Gazzetta Ufficiale Serie Generale n. 99 del 29 aprile 2010*);
g) Garante per la protezione dei dati personali: Provvedimento in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 (*Pubblicato in Gazzetta Ufficiale Serie Generale n. 300 del 24 dicembre 2008)*;
h) Garante per la protezione dei dati personali: "Lavoro: le linee guida per posta elettronica e internet" del 1 marzo 2007 (*Pubblicato in Gazzetta Ufficiale Serie Generale n. 58 del 10 marzo 2007).*

4. La conformità del trattamento dei dati personali al GDPR è dimostrata attraverso l'adozione di adeguate misure di sicurezza o attraverso l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato di cui al capo IV, sezione V, GDPR.

5. Il Titolare del trattamento ed i Soggetti Designati si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali, in conformità con quanto disposto dall'art. 29 GDPR e dall'art. 5 comma 3 del presente Regolamento.

Art. 10 - Registro delle attività di trattamento

1. Ai sensi dell'art. 30 GDPR ciascun/ciascuna Dirigente Capo Settore, designato/a con decreto del/della Sindaco/a ai sensi dell'art. 2-*quaterdecies* D.lgs. 196/2003, è responsabile della corretta tenuta del Registro delle attività di trattamento svolte per conto del Titolare nel proprio Settore di afferenza. Ciascun Registro reca le seguenti informazioni in ordine a tutti i trattamenti censiti dagli uffici del proprio Settore:

a) il nominativo ed i dati di contatto del Titolare del trattamento ovvero del Soggetto Designato nonché del DPO;
b) la base giuridica che rende lecito il trattamento;
c) le finalità del trattamento;
d) la descrizione delle categorie di interessati, nonché delle categorie di dati personali;
e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi gli eventuali destinatari di paesi terzi extra UE od organizzazioni internazionali;
f) l'eventuale presenza di un Responsabile del trattamento nominato ai sensi dell'art. 28 GDPR;
g) l'eventuale presenza di uno o più altri Titolari del trattamento, nel caso di trattamenti effettuati in regime di contitolarità ai sensi dell'art. 26 GDPR;
h) il termine previsto per la cancellazione dei dati personali;
i) la descrizione delle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 9 del presente Regolamento.

2. Il Registro è tenuto in forma digitale da ciascun Soggetto Designato ed è accessibile, attraverso applicativo informatico, dai soggetti della struttura organizzativa di afferenza opportunamente autorizzati, ai fini della registrazione di nuovi trattamenti o per l'aggiornamento dei trattamenti già censiti.

3. L'insieme aggregato dei Registri di Settore tenuti da ciascun Soggetto Designato costituisce, ai sensi dell'art. 30 GDPR, il Registro delle attività di trattamento del Titolare del trattamento.

Art. 11 - Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. La DPIA è una strumento che permette di realizzare e dimostrare la conformità di uno specifico trattamento che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche rispetto alla normativa vigente. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti a valutazione come redatti e pubblicati dal Garante ai sensi dell'art. 35 par. 4 - 6 GDPR.

2. Nel caso in cui un tipo di trattamento preveda l'uso di nuove tecnologie che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, svolge una valutazione dell'impatto del medesimo trattamento sulla protezione dei dati degli interessati ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso.

3. In particolare, la valutazione è richiesta qualora ricorrano, in conformità al comma successivo del presente articolo, i presupposti di cui all'art. 35 par. 3 GDPR, integrati dall'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto (Provvedimento del Garante per la

protezione dei dati personali dell'11 ottobre 2018, *Pubblicato in Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018*, e sue successive modificazioni ed integrazioni), ovverosia nei casi seguenti:

a) trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati ovvero lo svolgimento di attività predittive effettuate anche on-line o attraverso applicazioni, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti degli interessati;
b) trattamenti automatizzati finalizzati ad assumere decisioni che producono effetti giuridici oppure che incidono in modo significativamente analogo sugli interessati, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere;
c) trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio od il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso applicazioni, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative di varia natura;
d) trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata, o che incidono sull'esercizio di un diritto fondamentale oppure la cui violazione comporta un grave impatto sulla vita quotidiana degli interessati;
e) trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei/delle dipendenti;
f) trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
g) trattamenti effettuati attraverso l'uso di tecnologie innovative o di particolari misure di carattere organizzativo;
h) trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
i) trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento.

4. Nel caso in cui un trattamento risponda a due o più fattispecie tra quelle sopra indicate e tenuto comunque conto della probabilità concreta che un determinato evento costituisca un rischio elevato per i diritti e le libertà delle persone fisiche, in via generale occorre condurre una DPIA, salvo che il Titolare ritenga motivatamente che il trattamento non possa presentare un rischio elevato; altresì il Titolare può motivatamente ritenere che occorra comunque lo svolgimento di una DPIA per un trattamento che risponda anche solo ad una fattispecie di cui sopra.

5. Il Titolare garantisce lo svolgimento della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'ente. Per i trattamenti di competenza dei Settori, il Titolare affida la conduzione della DPIA a ciascun/ciascuna Dirigente Capo Settore in qualità di Soggetto Designato. Il Titolare ed i Soggetti Designati devono

consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA qualora ne ricorrano i presupposti; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Su richiesta, il DPO fornisce un parere in merito allo svolgimento della DPIA.

6. Il Titolare, in particolare, si consulta con il DPO in merito a quale metodologia adottare nello svolgimento della DPIA, su quali salvaguardie applicare a determinati trattamenti, comprese misure specifiche tecniche e organizzative di cui all'art. 32 GDPR per attenuare i rischi delle persone interessate, se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (ivi compresa la decisione se procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;

7. Il Responsabile e l'eventuale sub-responsabile del trattamento oggetto della DPIA, devono assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
Il Settore comunale competente e responsabile della sicurezza dei sistemi informatici dell'Ente fornisce supporto al Titolare per lo svolgimento della DPIA e può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

8. Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, fornendo un parere relativamente alla metodologia da adottare e sui rischi residuali individuati.

9. La DPIA non è necessaria nei casi seguenti:
   a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, par. 1 GDPR, considerato l'elenco delle tipologie di trattamento soggette a valutazione di cui al comma 3 del presente articolo;
   b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   c) se il trattamento è stato sottoposto a verifica da parte del Garante prima del 25 maggio 2018, data di entrata in vigore del GDPR, in condizioni specifiche che non hanno subito modifiche;
   d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

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

ii. della liceità del trattamento stabilita nei casi previsti dagli artt. 6, 9 e 10 GDPR, a seconda della tipologia di dati trattati, in combinato disposto con le pertinenti disposizioni del D.lgs. 196/2003;
iii. della adeguatezza e pertinenza dei dati raccolti rispetto alle finalità del trattamento stabilite da apposita base giuridica;
iv. del periodo limitato di conservazione dei dati personali;
v. delle informazioni fornite agli interessati;
vi. del diritto di accesso e portabilità dei dati;
vii. del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento degli interessati;
viii. dei rapporti con i Responsabili del trattamento nominati ai sensi dell'art. 28 GDPR;
ix. delle garanzie per gli eventuali trasferimenti di dati verso paesi extra UE od organismi internazionali;
x. di una eventuale necessità di consultazione preventiva del Garante;

c) valutazione dei rischi per i diritti e le libertà degli interessati, esaminando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singola tipologia di rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

11. Il Titolare raccoglie le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione deve essere specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

12. Il Titolare, in osservanza dell'art. 36 GDPR, deve consultare il Garante prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare può consultare il Garante anche nei casi in cui la vigente legislazione non stabilisce l'obbligo di consultare ed ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

13. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.
L'avvenuta effettuazione della DPIA svolta per determinati trattamenti, viene riportata nella scheda trattamento dati del corrispondente procedimento censito nel Registro delle categorie di attività di trattamento.

Art. 12 - Violazione dei dati personali

1. Per violazione dei dati personali (c.d. "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione

non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati.

2. Fatti salvi i casi in cui si possa ragionevolmente presumere che dalla violazione dei dati non possano derivare rischi per i diritti e le libertà degli interessati, il Titolare provvede alla notifica della violazione al Garante entro 72 ore e comunque senza ingiustificato ritardo dal momento in cui ne è venuto a conoscenza. Il Responsabile del trattamento, nominato ai sensi dell'art. 28 GDPR, è obbligato ad informare il Titolare della violazione senza ingiustificato ritardo, nonché deve assicurare al Titolare la massima collaborazione, fornendogli tutte le informazioni e gli strumenti necessari. Il Soggetto Designato del Settore presso cui è incardinata l'Unità organizzativa privacy di cui al successivo art. 15, è competente alla predisposizione e trasmissione della notifica al Garante ai sensi dell'art. 33 GDPR, previa consultazione con il DPO.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 GDPR, possono consistere in:

a) danni fisici, materiali o immateriali alle persone fisiche;
b) perdita del controllo dei dati personali;
c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale.
f) decifratura non autorizzata della pseudonimizzazione;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale (in particolare i dati sanitari e i dati giudiziari);
i) qualsiasi altro danno di natura economica o sociale significativo.

4. La notifica inoltrata al Garante per la protezione dei dati personali deve quantomeno contenere le informazioni essenziali di cui all'art. 33 par. 3 GDPR.

5. Qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvede ad informare gli interessati senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di far comprendere loro la natura della violazione dei dati personali verificatasi, ai sensi dell'art. 34 GDPR. Il Soggetto Designato del Settore coinvolto dal data breach è competente alla trasmissione di tale comunicazione, previa consultazione con il DPO.

6. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

a) coinvolgere un rilevante quantitativo di dati personali e/o di soggetti;
b) riguardare categorie particolari di dati personali di cui agli artt. 9 e 10 GDPR;
c) comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, dati finanziari, dati relativi alle abitudini e preferenze personali)
d) comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
e) impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate all'Autorità di controllo nazionale, nonché le circostanze ad esse relative, le conseguenze ed i provvedimenti adottati o quelli che intende adottare, se la violazione è in corso, per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza e può essere richiesta dal Garante al fine di verificare il rispetto delle disposizioni del GDPR. A tal fine, L'Unità organizzativa privacy custodisce ed aggiorna un registro contenente tutti gli eventi di violazione dei dati personali rilevati. Il registro è reso accessibile al DPO.

8. L'Unità organizzativa privacy predispone, aggiorna e porta a conoscenza dei Settori una più dettagliata procedura di gestione degli eventi di violazione dei dati personali, al fine di agevolare i flussi di comunicazione tra i Settori che dovessero rilevare un incidente di sicurezza nell'ambito della propria attività o per i trattamenti affidati a Responsabili del trattamento.

Art. 13 - Obbligo di informativa

1. In relazione a ciascun ambito di attività dell'Ente per cui sia prevista la raccolta di dati personali vi è obbligo in capo al Titolare di rendere l'informativa agli interessati che abbiano fornito direttamente i propri dati personali o per i quali i dati personali siano stati ottenuti indirettamente. Ciascun Soggetto Designato è tenuto a sovraintendere alla corretta redazione e somministrazione delle informative riferibili per materia ai propri uffici.

2. L'informativa deve essere allegata o richiamata dalla modulistica predisposta per il conferimento dei dati personali. Nel caso in cui la raccolta avvenga con altri mezzi, l'informativa deve essere comunque fornita all'interessato contestualmente all'atto stesso della raccolta dei dati. Qualora i dati non siano raccolti direttamente presso gli interessati, il Soggetto Designato provvede a somministrare l'informativa agli interessati nei modi e nei termini di cui all'art. 14 GDPR.

3. L'informativa può essere somministrata con modalità alternative e/o informatizzate, a condizione che ciò avvenga in conformità con il GDPR e le "Linee guida EDPB sulla trasparenza ai sensi del Regolamento 2016/679" adottate il 29 novembre 2017 ed emendate l'11 aprile 2018.

4. Ciascuna informativa, oltre ad essere chiara e concisa, deve contenere alcune informazioni essenziali che devono essere sempre comunicate o rese facilmente disponibili agli interessati, quali:

a) i dati di contatto del Titolare, con riferimento al Settore competente al trattamento;
b) i dati di contatto del DPO;
c) le finalità del trattamento cui sono destinati i dati personali raccolti;
d) la base giuridica che legittima il trattamento;
e) le categorie di destinatari dei dati personali, ivi compresi gli Uffici adibiti al trattamento medesimo, se individuabili;
f) il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

5. Gli ulteriori contenuti della informativa, a seconda che i dati siano stati ottenuti o meno direttamente dagli interessati, sono disciplinati rispettivamente dagli artt. 13 e 14 GDPR.

Art. 14 - Diritti degli interessati

1. Le persone fisiche, identificate od identificabili, le cui informazioni o dati personali sono trattati dal Titolare del trattamento o da altra persona, che tratta i dati per conto del Titolare del trattamento, hanno in qualunque momento il diritto di esercitare i diritti garantiti dal GDPR.
Ad esse deve essere consentito un agevole esercizio dei propri diritti tramite la possibilità di mettersi in contatto con il Settore competente al trattamento dei propri dati personali.

2. I diritti esercitabili nei confronti del Titolare, a seconda della natura e della finalità del trattamento, sono quelli di *accesso*, di *rettifica*, di *cancellazione*, di *limitazione di trattamento*, di *portabilità dei dati* e di *opposizione* (artt. 15 GDPR e seguenti). In qualsiasi ipotesi di trattamento gli interessati hanno diritto di proporre reclamo ad una Autorità di controllo ai sensi dell'art. 77 GDPR. Ciascun Soggetto Designato del Settore competente al trattamento per il quale è chiesto l'esercizio del diritto fornisce riscontro agli interessati nei tempi e modi previsti dall'art. 12 GDPR.

3. Restano ferme le limitazioni all'esercizio dei suddetti diritti direttamente previste dal GDPR o dal diritto nazionale o dell'Unione ai sensi dell'art. 23 GDPR.

4. L'Unità organizzativa privacy di cui al successivo art. 15, predispone, aggiorna e porta a conoscenza dei Settori una più dettagliata procedura di gestione delle istanze di esercizio dei diritti degli interessati al fine di rendere più agevole il flusso delle comunicazioni tra i Settori medesimi e di garantire l'effettivo soddisfacimento delle istanze presentate dagli interessati nei modi e nei tempi prescritti dalla normativa.

Art. 15 - Unità organizzativa privacy

1. Al fine di garantire gli adempimenti specificatamente previsti dal presente Regolamento, il Titolare del trattamento sovraintende alla costituzione di una Unità organizzativa privacy. L'Unità organizzativa privacy è istituita con provvedimento dirigenziale presso il Settore appositamente individuato dal Titolare e qualificato per la sua conoscenza specialistica, esperienza, capacità ed affidabilità in materia di protezione dei dati personali.

2. L'Unità organizzativa privacy si occupa della gestione ed assistenza traversale delle attività collegate agli adempimenti relativi alla protezione dati personali ai sensi della normativa vigente.

Art. 16 - Rinvio

1. Per tutto quanto non espressamente disciplinato nel presente Regolamento, si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti.

2. Il presente Regolamento abroga integralmente il Regolamento per il trattamento dei dati sensibili e giudiziari da parte del Comune di Padova approvato con deliberazione del Consiglio comunale n. 126 del 19 dicembre 2005, integrato con deliberazione del Consiglio comunale n. 110 del 13 dicembre 2006 e n. 17 del 12 marzo 2007.

Art. 17 - Entrata in vigore

1. Il presente Regolamento entra in vigore decorsi 15 giorni dalla pubblicazione dello stesso all'Albo Pretorio, da eseguirsi dopo l'esecutività della delibera che lo approva.