COMUNE DI GARGNANO

Provincia di Brescia

VERBALE DI ATTO DELLA GIUNTA COMUNALE
n° 20 del 25.03.2019

OGGETTO: Approvazione linee guida organizzative per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

L'anno **DUEMILADICIANNOVE** addì **VENTICINQUE** del mese di **MARZO** alle ore 17:30 nella sala delle adunanze presso la sede distaccata del Municipio sita a Gargnano in via Roma n. 28, si è riunita, su convocazione del Sindaco, la Giunta Comunale.
All'inizio della trattazione dell'argomento in oggetto risultano presenti i signori:

		Presente	Assente
Giovanni Albini	*Sindaco*	X	
Fernanda Bertella	*Vice Sindaco*		X
Giacomo Villaretti	*Assessore*	X	
Fiorenzo Razzi	*Assessore*	X	
Marino Piacenza	*Assessore*	X	
		4	1

Presiede il Sindaco signor Giovanni Albini il quale, essendo legale il numero dei presenti, dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.
Assiste il Segretario Comunale signor Graziano Cappa.

REFERTO DI PUBBLICAZIONE

Pubblicato all'albo pretorio telematico nel sito internet istituzionale di questo Comune, a decorrere dal - 6 MAG. 2019 per 15 giorni consecutivi e comunicato in pari data ai Capigruppo consiliari.

Addì - 6 MAG. 2019

L'istruttore direttivo – Servizio Segreteria

(Sergio Dallaguardi)

Copia conforme all'originale

☐ ed ai suoi allegati
☐ per estratto
☐ senza allegati

rilasciata per uso amministrativo, costituita da n° _____ fogli

Addì _____

L'istruttore direttivo – Servizio Segreteria

(Sergio Dallaguardi)

IMMEDIATA ESEGUIBILITA'

☒ Atto reso immediatamente eseguibile ai sensi dell'art. 134, comma 4 del D.Lgs. n. 267/2000

Addì - 6 MAG. 2019

L'istruttore direttivo – Servizio Segreteria

(Sergio Dallaguardi)

CERTIFICATO DI ESECUTIVITA'

Atto esecutivo ai sensi dell'art. 134, comma 3 del D.Lgs. n. 267/2000 in data _____.

Pervenute opposizioni durante la pubblicazione all'albo pretorio

☐ sì
☐ no

Addì _____

L'istruttore direttivo – Servizio Segreteria

(Sergio Dallaguardi)

OGGETTO: Approvazione linee guida organizzative per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

LA GIUNTA COMUNALE

VISTA la proposta di deliberazione allegata, corredata dai pareri in ordine alla regolarità tecnica ed alla regolarità contabile, rilasciati dai competenti responsabili di servizio ai sensi dell'art. 49, comma 1, del Testo Unico approvato con D.Lgs. n. 267 del 18 agosto 2000;

Con voti favorevoli unanimi, espressi in forma palese per alzata di mano,

D E L I B E R A

1) di approvare l'allegata proposta di deliberazione con oggetto "**Approvazione linee guida organizzative per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**".

Con successiva votazione in forma palese per alzata di mano, dalla quale si rilevano voti favorevoli unanimi,

D E L I B E R A

2) di dichiarare la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs. n. 267 del 18 agosto 2000.

Letto, confermato e sottoscritto

Il Sindaco
(Giovanni Albini)

Il Segretario Comunale
(Graziano Cappa)

COMUNE DI GARGNANO (Brescia)

COMUNE DI GARGNANO

Provincia di Brescia

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE
in seduta del 25 marzo 2019

OGGETTO: Approvazione linee guida organizzative per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

PRESO ATTO che:
- il Parlamento Europeo ed il Consiglio in data 27.04.2016 hanno approvato il Regolamento UE 679/2016 (GDPR – General Data Protection Regulation o RGPD – Regolamento Generale Protezione Dati) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, regolamento che abroga la direttiva 95/46/CE mirando a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione Europea;
- come disposto dall'art. 99 del RGPD, pubblicato nella Gazzetta Ufficiale dell'Unione Europea in data 04.05.2016, il Regolamento è direttamente applicabile in tutti gli stati membri dell'Unione Europa a decorrere dal 25.05.2018 e non richiede alcuna forma di legislazione attuativa specifica a livello nazionale;
- al predetto RGPD sono state apportate alcune rettifiche contenute nel documento pubblicato sulla Gazzetta Ufficiale dell'Unione Europea in data 23.05.2018;

VISTO il D.Lgs. n. 101 del 10.08.2018, entrato in vigore in data 19.09.2018, emanato in attuazione dell'art. 13 della legge n. 163 del 25.10.2017, con il quale sono state introdotte nuove disposizioni per l'adeguamento della normativa nazionale ai contenuti del RGPD;

VISTA la Guida predisposta dal Garante per la protezione dei dati personali circa la corretta applicazione della normativa e consultabile sul relativo sito internet dell'Autorità, con la quale viene offerto un panorama delle principali problematiche che imprese e soggetti pubblici devono tenere presenti in materia di protezione dei dati personali;

RILEVATO che:
- le norme introdotte dal RGPD si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;
- appare quanto mai necessario ed opportuno definire modalità organizzative, misure procedimentali e regole di dettaglio finalizzate anche ad omogeneizzare questioni interpretative, che permettano all'Ente di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni del Regolamento UE;

RITENUTO pertanto opportuno procedere alla definizione di linee guida che consentano a questa Amministrazione di provvedere all'adattamento dell'organizzazione alle disposizioni contenute nel Regolamento UE 2016/679, chiarendo e disciplinando gli aspetti rimessi alla propria autonomia organizzativa e procedimentale;

VISTO l'allegato documento contenente le linee guida organizzative per l'attuazione del RGPD, predisposto con il supporto del Responsabile della Protezione dei Dati, designato con propria deliberazione n. 50 in data 06.08.2018;

RITENUTE tali linee guida conformi alle norme in materia ed adeguate alle caratteristiche dell'ente e quindi meritevoli di approvazione;

RITENUTO che il presente atto sia di competenza della Giunta Comunale, trattandosi dell'approvazione di un documento attinente l'attività organizzativa interna all'ente, ai sensi dell'art. 48 del D.Lgs. n. 267/2000;

SI PROPONE ALLA GIUNTA COMUNALE

1) di approvare l'allegato documento contenente le linee guida organizzative per l'attuazione delle norme contenute nel Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

2) di disporre la pubblicazione delle linee guida approvate all'interno del sito internet istituzionale di questo Comune, sia nella sezione "Amministrazione trasparente" che nell'apposita pagina informativa dedicata alla privacy;

3) di rendere nota l'adozione delle linee guida agli Uffici comunali mediante comunicazione interna in modalità telematica;

4) di trasmettere copia della deliberazione di approvazione delle presente proposta al Responsabile della Protezione dei Dati personali;

5) di dichiarare immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs. n. 267 del 18 agosto 2000, la deliberazione di approvazione della presente proposta.

Addì 25 marzo 2019

Il Sindaco
(Giovanni Albini)

Pareri ai sensi dell'art. 49, comma 1 del D.Lgs. n. 267 del 18 agosto 2000
Per la regolarità tecnica: **favorevole** Addì 25 marzo 2019 Il responsabile del Servizio (Giovanni Albini)
Parere di regolarità contabile: **favorevole** Addì 25 marzo 2019 Il responsabile del Servizio Economico Finanziario (Giovanni Albini)

COMUNE DI GARGNANO

Provincia di Brescia

OGGETTO: Approvazione linee guida organizzative per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Allegati:

- Linee guida organizzative;

Allegato alla deliberazione della Giunta Comunale n° 20 del 25 marzo 2019

Il Sindaco
(Giovanni Albini)

Il Segretario Comunale
(Graziano Cappa)

COMUNE DI GARGNANO

Provincia di Brescia

LINEE GUIDA ORGANIZZATIVE PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Approvate con deliberazione della Giunta Comunale n. 20 in data 25 marzo 2019

Art. 1 Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Gargnano (BS).

Art. 2 Titolare del trattamento

1. Il Comune di Gargnano, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può delegare i relativi compiti a funzionari in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei princìpi applicabili al trattamento di dati personali stabiliti dall'art. 5 del RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i princìpi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli da 15 a 22 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa, di bilancio e di PEG, 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.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

   a) le informazioni indicate dall'art. 13 del RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

   b) le informazioni indicate dall'art. 14 del RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 del RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 10.

6. Il Titolare, inoltre, provvede a:

   a) designare gli incaricati interni del trattamento nelle persone operanti nelle singole strutture in cui si articola l'organizzazione comunale, che sono autorizzati a compiere operazioni di trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

   b) nominare il Responsabile della protezione dei dati (RPD) – Data Protection Officer (DPO);

c) nominare quale Responsabile del trattamento (ai sensi dell'articolo 28 del RGDP) i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni all'ente 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 e predisporre il relativo elenco;

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 3 Presupposti di liceità del trattamento

1. I trattamenti sono compiuti dal Comune sulla base dei seguenti presupposti di liceità:

   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

      Rientrano in questo ambito i trattamenti compiuti per:

      - 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;
      - la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
      - l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

      La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.

   b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

   c) l'esecuzione di un contratto con soggetti interessati.

   d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4 Organizzazione interna del Titolare del trattamento – Incaricati

1. Il Titolare del trattamento individua gli incaricati al trattamento intesi come persone fisiche autorizzate a compiere operazioni di trattamento. I soggetti individuati come incaricati al trattamento sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono disciplinati:

- l'elenco dei trattamenti, la durata dell'incarico, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- le modalità di esecuzione dell'incarico.

Tale disciplina può essere contenuta anche in idoneo atto giuridico da stipularsi fra il Titolare e ciascun incaricato.

Art. 5 Responsabili esterni del trattamento

1. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento (ai sensi dell'art. 28 del RGDP), forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
2. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, del RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
3. È consentita la nomina di sub-responsabili da parte di ciascun Responsabile per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.
4. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
5. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge ed a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
   - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
   - all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
   - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
   - alla designazione del Responsabile per la Protezione dei Dati (RPD), se previsto dalla legge;
   - ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;

- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 6 Responsabile della protezione dati – Data Protection Officer

1. Il Responsabile della protezione dei dati - Data Protection Officer (in seguito indicato con "RPD") è individuato nella figura unica di un professionista, in possesso di comprovate conoscenze specialistiche in materia di protezione dei dati, da individuare tramite procedura da espletare nel rispetto delle disposizioni vigenti in materia di appalti pubblici.

   Il RPD è incaricato dei seguenti compiti:

   a) informare e fornire consulenza al Titolare ed ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

   b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare;

   c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare;

   d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

   e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare al Garante;

   f) altri compiti e funzioni a condizione che il Titolare si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

2. Il Titolare assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

   - il RPD è invitato a partecipare alle riunioni di coordinamento che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. Nello svolgimento dei compiti affidatigli il RPD 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 RPD:
   a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare.
4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuitigli, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.
5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:
   - il Responsabile per la prevenzione della corruzione e per la trasparenza;
   - qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
6. Il Titolare fornisce al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:
   - supporto attivo per lo svolgimento dei compiti da parte del personale di natura amministrativa e degli organi di natura politica, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa, di bilancio e di Piano della performance;
   - tempo sufficiente per l'espletamento dei compiti affidati al RPD;
   - supporto adeguato in termini di risorse finanziarie, di infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, di personale;
   - comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
   - accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il RPD non può essere rimosso o penalizzato dal Titolare e da un Responsabile esterno del trattamento per

l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare o suo delegato. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare.

Art. 7 Sicurezza del trattamento

1. Il Comune di Gargnano e ciascun Responsabile esterno del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento possono ricomprendere, se del caso: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate:

   - sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus, firewall, antintrusione, altro);

   - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Il Comune di Gargnano e ciascun Responsabile esterno del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare e del Responsabile della protezione dati – Data Protection Officer sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" se presente.

Art. 8 Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

   a) il nome ed i dati di contatto dell'Ente, del Rappresentante legale e/o del suo Delegato ai sensi del precedente art. 2, eventualmente del Contitolare del trattamento, del RPD;

   b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 7.

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa dell'Ente in forma telematica o cartacea.

Art. 9 Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate dall'Ente in qualità di Responsabile esterno di un Titolare del trattamento terzo conterrà le seguenti indicazioni:

   a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento e del RPD;

   b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

   c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

   d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 7.

2. Il registro è tenuto dall'Ente presso i propri uffici.

Art. 10 Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, del RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, del RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

   a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del RGDP;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

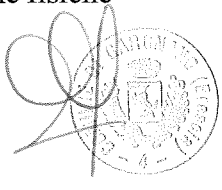
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto. Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non possa presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione 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. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. Il Responsabile esterno del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

   - se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, del RGDP;



- 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;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RPD e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

   a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

   b) valutazione della necessità e proporzionalità dei trattamenti, sulla base: delle finalità specifiche, esplicite e legittime; della liceità del trattamento; dei dati adeguati, pertinenti e limitati a quanto necessario; del periodo limitato di conservazione; delle informazioni fornite agli interessati; del diritto di accesso e portabilità dei dati; del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento; dei rapporti con i responsabili del trattamento; delle garanzie per i trasferimenti internazionali di dati; consultazione preventiva del Garante privacy;

   c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

   d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

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

10. 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.

Art. 11 Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*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 dall'Ente.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile esterno del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti, discriminazione;
   - furto o usurpazione d'identità;
   - perdite finanziarie, danno economico o sociale;
   - decifratura non autorizzata della pseudonimizzazione;
   - pregiudizio alla reputazione;
   - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie particolari di dati personali;
   - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   - 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);
   - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art. 12 Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.