COPIA

UNIONE DEI COMUNI

"ARO 2 Barletta Andria Trani"

Deliberazione della Giunta

Nr. 26

OGGETTO: Adozione del Regolamento interno per la protezione delle persone fisiche con riguardo al trattamento dei dati personali – Regolamento UE 2016/679.

L'anno duemila **diciotto** il giorno **ventinove** del mese di **novembre** alle ore **12.40** in Andria, presso la Sala Giunta della Sede Municipale, si è riunita, previa convocazione trasmessa ai Sindaci, componenti dell'ARO2, la Giunta dell'Unione dei Comuni dell'ARO2.

Risultano presenti ed assenti i sotto indicati componenti :

Comune	*Presenti*	*Assenti*	*Rappresentante*
Andria	*1*		*Nicola GIORGINO – Sindaco*
Canosa di Puglia	*2*		*Roberto MORRA - Sindaco*
Minervino Murge	*3*		*Maria Laura MANCINI - Sindaco*
Spinazzola	*4*		*Michele PATRUNO - Sindaco*

Assume la presidenza l'avv. Nicola GIORGINO, Presidente dell'ARO2, il quale, preso atto della validità della adunanza - regolarmente convocata con nota prot. 1315 del 22/11/2018, dichiara aperta la seduta.

Partecipa per le funzioni verbalizzanti il Segretario Generale Dott. Giuseppe Borgia.
Sono presenti i Dirigenti dell'ARO Dott.ssa Maria De Palma e Ing. Antonio Dibari.

LA GIUNTA DELL'UNIONE

PRESO ATTO che :

- il Parlamento europeo ed il Consiglio in data 27.4.2016 hanno approvato il Regolamento UE 679/2016 (GDPR- *General Data Protection Regulation)* relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

- il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri;

- il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presenti in vista della piena applicazione del Regolamento, prevista il 25 maggio 2018;

- ai sensi dell'art.13 della Legge n.163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27 aprile 2016 di che trattasi;

- in data 19/09/2018 è entrato in vigore il Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";

RILEVATO che :
- le norme introdotte dal Regolamento UE 2016/679 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 entro il 25 maggio 2018;

- appare necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano di agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;

Visto lo schema di Regolamento allegato;

RITENUTO pertanto opportuno procedere alla sua approvazione per permettere a questa Unione di Comuni denominata "ARO 2 Barletta Andria Trani" di provvedere con immediatezza all'attuazione del Regolamento UE 2016/679;

Tanto premesso,

Acquisito il parere di regolarità tecnica espresso ai sensi dell'art. 49 c. 1 D.Lg 267/2000;

Con voti unanimi favorevoli

DELIBERA

- Di approvare il Regolamento interno per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, allegato al presente atto per costituirne parte integrante e sostanziale.

Regolamento interno per la protezione delle persone fisiche con riguardo al trattamento dei dati personali

INDICE

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, nell' Unione di Comuni denominata "ARO 2 Barletta Andria Trani" (d'ora in avanti ARO).

Art. 2 – Titolare del trattamento

1. L'ARO , rappresentato ai fini previsti dal RGPD dal Presidente 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 Presidente può delegare le relative funzioni a soggetti interni, in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 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 principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

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

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

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

2. 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 "VIP") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto
conto di quanto indicato dal successivo art. 9.

3. Il Titolare, inoltre, provvede a:

a) nominare il Responsabile della protezione dei dati;

b) designare, facoltativamente, i "Delegati interni per la protezione dei dati" nelle persone che sono preposte al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

c) nominare quale Responsabile del trattamento, ai sensi dell'art. 28 del RGPD, i soggetti pubblici o privati affidatari di attività e servizi per conto dell'ARO, relativamente alle banche dati gestite da soggetti esterni all'ARO 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;

4. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'ARO 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 RGPD**. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di protezione dei dati personali, 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 specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.
5. L'ARO 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 – Finalità del trattamento

1. I trattamenti sono compiuti dall'ARO per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per la gestione delle attività di servizio rifiuti, comprensivo di spazzamento, raccolta e trasporto dei rifiuti urbani ed assimilati, al fine di raggiungere i seguenti obiettivi:

- semplificazione amministrativa
- razionalizzazione delle risorse
- ottimizzazione dei servizi offerti
- contenimento dei costi complessivi
- massimizzazione delle sinergie
- valorizzazione delle professionalità.

b) l'adempimento di obblighi legali al quale è soggetto L'ARO. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
c) l'esecuzione di contratti con soggetti Terzi.

Art. 4 – Responsabile del trattamento

1. Facoltativamente, è nominato il "Delegato interno per la protezione dei dati" con riferimento al trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il "Delegato per la protezione dei dati" 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. 6 rivolte a garantire che i trattamenti dell'ARO siano effettuati in conformità al RGPD.
2. i "Delegati interni per la protezione dei dati" sono designati, di norma, mediante atto del Presidente, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

3. l 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 RGPD,

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.

4. 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, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento 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 specificatamente 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 dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

6. Il Responsabile del trattamento (soggetto esterno all'ARO) 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.

7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e 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 a ciò demandato dal Titolare;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "VIP") 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 all' Autorità Garante, 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. 5 – Responsabile della protezione dei dati

1. Il Responsabile della protezione dei dati è designato dal Titolare in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Regolamento UE 2016/679, che di seguito sono elencati :

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché 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 e/o al Responsabile del trattamento 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 e del Responsabile del trattamento. 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 e del Responsabile del trattamento;

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

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione

dei dati (VIP) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a:

- se condurre o meno una VIP;
- quale metodologia adottare nel condurre una VIP;
- se condurre la VIP con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate;
- se la VIP 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 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) (eventuale) la tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino 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 ed il Responsabile del trattamento assicurano 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 dei Dirigenti/Responsabili P.O. 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 ed al Responsabile del trattamento.

4. Il RPD 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'ARO.

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;
- il Responsabile del trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il Titolare ed il Responsabile del trattamento forniscono 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:

- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, 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'ARO;
- accesso garantito ai settori funzionali dell'ARO 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 dal Responsabile 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, oppure al Responsabile del trattamento. 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 ed al Responsabile del trattamento.

Art. 6 – Sicurezza del trattamento

1. L'ARO e ciascun eventuale "Delegato interno per la protezione dei dati", 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 ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi 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, con il supporto dell'Amministratore di sistema per gli aspetti tecnologici (figura interna o esterna all'ARO), le seguenti:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; registrazione accessi etc..);
- 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. L'ARO e ciascun eventuale "Delegato per la protezione dei dati" 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 sono pubblicati sul sito istituzionale dell'ARO all'indirizzo www.unionearo2bt.it.

Art. 7 – Registro delle attività del 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'ARO e del Presidente, ai sensi del precedente art.2, eventualmente del Contitolare del trattamento e del Responsabile della protezione dei dati;
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.6.

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'ARO, in forma telematica/cartacea.

3. Il Titolare del trattamento può decidere di affidare al Responsabile della protezione dei dati (RPD) il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

Art. 8 – Valutazione di impatto Privacy

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 (VIP) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La VIP 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 VIP si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante, ai sensi dell'art. 35, pp. 4-6, RGDP.

3. La VIP 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, 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, 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'ARO, 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 VIP, salvo che il Titolare ritenga motivatamente che non può 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 VIP.

4. Il Titolare garantisce l'effettuazione della VIP ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della VIP ad un altro soggetto, interno o esterno all'ARO.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la VIP; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della VIP. Il RPD monitora lo svolgimento della VIP.

Il Responsabile del trattamento deve assistere il Titolare nella conduzione della VIP 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 VIP.

5. Il RPD può proporre lo svolgimento di una VIP 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 VIP in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La VIP 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, 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 VIP. In questo caso si possono utilizzare i risultati della VIP svolta per l'analogo trattamento;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una VIP all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una VIP per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica.

7. La VIP 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;

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 specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il Titolare deve consultare il Garante prima di procedere al trattamento se le risultanze della VIP condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante 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 VIP 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. 9 – 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'ARO.

2. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Ciascun eventuale "Delegato interno per la protezione dei dati" e dipendente dell'ARO informa il Presidente, anche per il tramite del Responsabile della protezione dei dati, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Il Titolare, con il supporto del Responsabile della protezione dei dati, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La notifica della violazione è effettuata tramite posta elettronica certificata del Titolare del trattamento con l'invio del modello *data-breach* all'Autorità Garante per la protezione dei dati personali, all'indirizzo email databreach.pa@pec.gpdp.it.

3. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni :

a) la natura della violazione dei dati
b) i dati di contatto del Responsabile della protezione dei dati
c) le possibili conseguenze della violazione
d) le misure adottate o di cui si propone l'adozione per porvi rimedio

Non è richiesta la comunicazione all' interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui sopra è soddisfatta.

5. Nel caso di violazione dei dati personali il Titolare del trattamento procede con una valutazione complessiva dell'impatto sui diritti e libertà degli interessati in considerazione della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento.

6. I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

7. Il Titolare, con il supporto del Responsabile della protezione dei dati, verifica se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali ed informa tempestivamente il Garante e l'interessato, se del caso.

8. A seguito valutazione preliminare della violazione, il Titolare del trattamento con il supporto del Responsabile della protezione dei dati, adotta una le seguenti azioni :

a) se dalla violazione risulta probabile che possano derivare rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento;
b) se dalla violazione risulta probabile che possano derivare elevati rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data-breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/679, secondo le previsioni di cui all'articolo 2 del presente Regolamento e alla comunicazione della violazione ai soggetti interessati ai sensi dell'art. 34 del Regolamento UE 2016/679;
c) ove non risulti probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procede con le notifiche e comunicazioni di cui ai p.ti a) e b).

Pertanto, il Titolare del trattamento è esentato dalla notifica della violazione solo se è in grado di dimostrare al Garante che il *data-breach* non presenta rischi per i diritti e le libertà fondamentali delle persone fisiche interessate.

9. Ogni eventuale "Delegato per la protezione dei dati" o dipendente dell'ARO ha l'obbligo di segnalare senza ingiustificato ritardo, entro 24 ore, la violazione dei dati rilevata ai soggetti di seguito elencati :

- Presidente
- Responsabile della protezione dei dati

La segnalazione, in prima istanza, può essere effettuata in qualsiasi forma, anche per le vie brevi e successivamente formalizzata tramite invio di posta elettronica o atto interno da

protocollare. A tal fine è reso disponibile un modello per la segnalazione, ad uso interno, che si allega al presente Regolamento per farne parte integrante e sostanziale.
Ai fini dell'osservanza dei tempi imposti dal Regolamento Ue 2016/679, il Titolare del trattamento dei dati, provvederà a convocare, non oltre 24 ore dalla rilevazione della violazione, una riunione con i soggetti di seguito elencati :

- Presidente
- Responsabile della protezione dei dati
- Amministratore di Sistema (interno o esterno)

Il Responsabile della protezione dei dati ha facoltà di convocare altri soggetti ritenuti necessari per la valutazione della gravità della violazione dei dati.

Il Responsabile della protezione dei dati è tenuto a documentare l'intera attività istruttoria, acquisendo tutte le informazioni necessarie per la registrazione dell'evento e per la notificazione al Garante, ove necessario.
A conclusione della valutazione della violazione, il Responsabile della protezione dei dati predispone un verbale, sottoscritto da tutti i convenuti e protocollato, che sarà inoltrato al Titolare del trattamento per i conseguenti adempimenti.

10. Il Titolare del trattamento documenta le violazioni dei dati in apposito registro elettronico da esibire in caso di accertamento ispettivo dell'Autorità.
Il registro delle violazioni è custodito dal Responsabile della protezione dei dati con la massima diligenza e nell'osservanza del Regolamento UE 2016/679.

11. Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del Regolamento UE 2016/679, ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto al Garante, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri.

Il Titolare del trattamento o il Responsabile del trattamento è tenuto a risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento UE 2016/679 ma è esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
La violazione delle disposizioni contenute nel Regolamento 2016/679 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro.

Art. 10 – Rinvio

Per quanto non espressamente previsto nel presente Regolamento si fà rinvio al Regolamento UE 679/2016 e successive regolamentazioni.
Il Titolare del trattamento si riserva di modificare e integrare il presente Regolamento, ove ritenuto necessario, anche alla luce di eventuali successive innovazioni normative o pronunciamenti dell'Autorità Garante per la protezione dei dati.

Art. 11 – Allegati

Si allega al presente Regolamento :
- il modello per la segnalazione di violazioni dei dati *(c.d. data-breach)* ad uso interno

ALLEGATO ALLA PROPOSTA DI

DELIBERAZIONE DI GIUNTA DELL'UNIONE

avente ad

OGGETTO: Adozione del Regolamento interno per la protezione delle persone fisiche con riguardo al trattamento dei dati personali – Regolamento UE 2016/679

PARERI DI REGOLARITA' AI SENSI DELL'ART. 49 del D.Lg.vo n° 267/2000

****

Ai sensi dell'art. 49, 1° comma del D.Lg.vo n° 267/2000, sulla presente proposta si esprime il seguente parere sotto il profilo della **REGOLARITA' TECNICA**:

favorevole

Lì, 19/09/18

IL RESPONSABILE DEL SERVIZIO
f.to Dott.ssa Maria De Palma

Del che si è redatto il presente verbale che, previa lettura e conferma, viene sottoscritto.

IL PRESIDENTE
F.to avv. Nicola GIORGINO

IL SEGRETARIO VERBALIZZANTE
F.to Dott. Giuseppe Borgia

Copia conforme all'originale, in carta libera per uso amministrativo.

Li, 13 DIC. 2018

UNIONE DI COMUNI ARO 2 BT

IL SEGRETARIO GENERALE
Dott. Giuseppe BORGIA

Prot. N. _____

Della suestesa deliberazione viene iniziata oggi la pubblicazione all'Albo del Comune di _____ per 15 giorni consecutivi.

Addì 13 DIC. 2018

UNIONE DI COMUNI ARO 2 BT

IL SEGRETARIO GENERALE

IL SEGRETARIO GENERALE
Dott. Giuseppe BORGIA

ADEMPIMENTI RELATIVI ALLA PUBBLICAZIONE

Il Responsabile del procedimento, visti gli atti d'ufficio

ATTESTA

Che la presente deliberazione:

> è stata affissa all'Albo Pretorio comunale per 15 giorni consecutivi a partire dal _____ al _____ come prescritto dall'art. 124 comma 1°, del D.Lg.vo n° 267 del 18/8/2000.

> è divenuta esecutiva perchè:

- decorsi 10 giorni dalla pubblicazione (art. 134 comma 3) del D.Lg.vo n° 267 del 18/8/2000
- dichiarata immediatamente eseguibile (art. 134 comma 4) del D.Lg.vo n° 267 del 18/8/2000.

_____ _____

Addi'

_____