COMUNE DI PESCANTINA

PROVINCIA DI VERONA

REGOLAMENTO SULLA PROTEZIONE DEI DATI PERSONALI

INDICE

Art. 1 Oggetto

1. Il presente Regolamento ha per oggetto l'individuazione dei principi e degli strumenti finalizzati ad attuare in modo funzionale ed efficace la normativa sulla *privacy* relativa alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nel Comune di Pescantina.

2. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del Regolamento europeo (*General Data Protection Regulation* del 27 aprile 2016 n. 679, indicato con "*RGPD*", Regolamento Generale Protezione Dati), del Decreto legislativo n. 196 del 2003 (per le norme non abrogate o modificate dal Decreto legislativo n. 101 del 2018) e del Decreto Legislativo 10 agosto 2018, n. 101, 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), e la relativa normativa di attuazione.

Art. 2 Titolare del trattamento

1. Il Comune di Pescantina (di seguito indicato con "*Titolare*"), rappresentato ai fini previsti dalla normativa sulla *privacy* dal Sindaco pro-tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee. Il Sindaco può delegare le relative funzioni a Dirigente 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 e dall'art. art. 2 quater del D.Lgs. n. 101/2018: liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

3. Il Titolare deve assicurare l'adozione delle misure tecniche e organizzative adeguate e deve essere in grado di dimostrare che il trattamento è effettuato conformemente alla normativa in materia di protezione dei dati personali.

4. 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 del RGPD e dall'art. 2-undecies del D.Lgs. n. 101/2018, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

5. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), 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.

6. 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 siano stati ottenuti presso lo stesso interessato.

7. 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 RGPD, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 10.

8. È inoltre di competenza del Titolare:

a. adottare tutti gli interventi necessari, con riferimento alle disposizioni della normativa in materia di protezione dei dati personali;

b. nominare il Responsabile della protezione dei dati personali;

c. incaricare i Dirigenti delle singole strutture in cui si articola l'organizzazione comunale, quali preposti al trattamento dei dati personali esistenti nelle articolazioni organizzative di loro competenza;

d. nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente ai dati che detti soggetti gestiscono per conto del 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 funzioni istituzionali. Il Titolare può delegare il compito di nominare i Responsabili del trattamento ai singoli dirigenti, per gli ambiti di competenza del settore di appartenenza;

e. assicurare l'adeguata formazione dei soggetti autorizzati al trattamento dei dati personali.

9. Il Titolare deve inoltre costituire nell'ambito dell'organizzazione dell'Ente un'apposita struttura interna, come previsto dall'art. 8, comma 1, e assegnare a detta struttura adeguati mezzi sia in termini di personale che di risorse.

10. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da altri Enti ed organismi statali o regionali, mediante accordo, si realizza la contitolarità di cui all'art. 26 RGPD. Con specifico accordo si definiscono 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 articoli 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.

11. Il Comune di Pescantina 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 effettuati dal Comune di Pescantina per le seguenti finalità:

a) per 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, in particolare 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) per l'adempimento di un obbligo legale al quale è soggetto il Comune di Pescantina. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.

c) per 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. Soggetti e responsabilità

1. Ciascun Responsabile di area, compreso il Segretario Generale, coordina, in qualità di designato, le attività di trattamento dei dati personali esistenti nell'articolazione organizzativa di rispettiva competenza, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 volte a garantire che i trattamenti siano effettuati in conformità al RGPD.

2. La designazione avviene, di norma, mediante decreto del Sindaco, nel quale sono tassativamente disciplinati:

A. la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;

B. il tipo di dati personali oggetto di trattamento e le categorie di interessati;

C. gli obblighi ed i diritti del Titolare del trattamento.

3. Il personale assegnato agli uffici dell'Ente svolge le funzioni di soggetto incaricato con provvedimento del responsabile di Area e attribuzione in relazione ai trattamenti e ai poteri/doveri previsti dal proprio ruolo organizzativo e nel rispetto delle indicazioni e istruzioni formali e/o informali fornite dal responsabile medesimo.

Art. 5 Responsabile del trattamento

1. Il Titolare può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati (Responsabile del trattamento) che vi siano tenuti a seguito di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge. Ai fini della scelta del soggetto con il quale contrarre, il Comune deve anche valutare l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto, affinché lo stesso sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Ai sensi dell'art. 2, comma 8, Il Titolare può delegare il compito di nominare i Responsabili del trattamento ai singoli responsabili di area, per gli ambiti di competenza del settore di appartenenza.

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, 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 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 sub responsabili che operano sotto la diretta autorità del Responsabile, attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

4. 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.

5. 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, fermo restando il dovere di riservatezza che grava in capo a ciascun dipendente dell'Amministrazione Comunale.

6. 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, ed in particolare:

a. alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;

b. all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;

c. alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

d. 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;

e. ad informare il Titolare, senza ingiustificato ritardo, dei 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 (RPD)

1. Il Responsabile della Protezione dei Dati (in seguito indicato con "*RPD*") può essere individuato in un dipendente a tempo indeterminato del Comune di Pescantina, che non sia responsabile di area designato al trattamento dei dati, oppure in un soggetto esterno (professionista o persona giuridica) in possesso di tutte le qualità professionali atte a

ricoprire il ruolo. In particolare il RPD deve possedere una comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali, nonché un'adeguata capacità di promuovere la diffusione di una cultura della protezione dei dati personali all'interno dell'organizzazione comunale, favorendo la formazione del personale attraverso la proposta di piani di aggiornamento periodico.

2. Il Responsabile della Protezione dei Dati in particolare:

a. informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;

b. sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c. coopera con il Garante per la protezione dei dati personali;

d. funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del RGPD, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;

e. partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del servizio ICT competente o ne richiede di specifiche;

f. promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;

g. partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;

3. La figura di RPD è incompatibile con chi determina le finalità o i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

A. il Responsabile per la prevenzione della corruzione e per la trasparenza;

B. il Responsabile del trattamento;

C. qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

4. II Titolare o suo delegato, i dirigenti designati e i Responsabili del trattamento forniscono al RPD le informazioni e la collaborazione necessarie per lo svolgimento dei compiti di riferimento e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

a. supporto attivo per lo svolgimento dei compiti da parte del Titolare o suo delegato, dei dirigenti designati, della Giunta Comunale e dei Responsabili del Trattamento, anche considerando l'attuazione delle attività necessarie per la protezione e la messa in sicurezza dei dati nell'ambito della programmazione operativa (DUP), di bilancio, di PEG;

b. tempo sufficiente per l'espletamento dei compiti affidati al RPD;

c. supporto adeguato in termini di risorse finanziarie, umane, infrastrutture (sede, attrezzature, strumentazione), con la costituzione di apposita struttura interna, come previsto dall'art. 2, comma 9;

d. 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;

e. accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

5. 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.

6. Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti.

7. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare — Sindaco o suo Delegato - del trattamento.

8. 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 o suo delegato e ai Responsabili del trattamento.

Art. 7 Sicurezza del trattamento

1. Il Sindaco pro-tempore in qualità di Titolare e ciascun responsabile di area designato collaborano con il RPD per attuare le misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e delle risorse a disposizione per coprire i costi di attuazione, nonché rispetto alla natura, al campo di applicazione, al contesto e alle finalità del trattamento, anche in considerazione del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (distruzione, perdita, modifica, divulgazione non autorizzata o accesso in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati).

2. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento (fase realizzativa).

3. 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.

4. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Settore cui è preposto ciascun dirigente:

a. procedure, *policy* e regolamento comunale per la sicurezza e l'utilizzo delle risorse informatiche e telematiche;

b. sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione (antivirus, firewall, sistemi anti-intrusione informatica, altro);

c. misure antincendio, sistemi di rilevazione di intrusione, sistemi di sorveglianza, sistemi di protezione con videosorveglianza, registrazione accessi; porte, armadi e contenitori ignifughi dotati di serrature, sistemi di copiatura e conservazione di archivi elettronici;

d. altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

5. La conformità del trattamento dei dati 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.

6. Il Comune di Pescantina e ciascun dirigente designato, con il supporto del RPD, forniscono adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

7. I nominativi ed i dati di contatto del Titolare e del RPD sono pubblicati sul sito istituzionale del Comune di Pescantina.

8. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati particolari (sensibili) per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (*ex* articoli 20 e 22, D.Lgs. n. 193/2006).

Art. 8 Strutture competenti in materia di *privacy* e sistemi informativi.

1. È costituita nell'ambito dell'organizzazione dell'Ente un'apposita struttura interna adeguatamente dotata di personale e di risorse, competente per le seguenti attività:

a. dare supporto al Responsabile per la Protezione dei dati personali;

b. svolgere compiti di coordinamento e supporto degli uffici dell'Ente al fine di assicurare l'applicazione delle disposizioni in materia di trattamento dei dati personali;

c. effettuare apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compresi i profili relativi alla sicurezza informatica, in collaborazione con il Responsabile della protezione dati;

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

e. svolgere verifiche sulla puntuale osservanza della normativa e delle policy del Comune in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del RPD e realizza le verifiche specifiche richieste dallo stesso;

f. promuovere la formazione di tutto il personale dell'Ente in materia di sicurezza dei dati, anche attraverso un piano di comunicazione e divulgazione all'interno dell'Ente, coordinandosi con le azioni promosse dal RPD;

g. supportare gli uffici nella gestione delle istanze presentate dagli interessati al trattamento di dati personali.

2. Al responsabile/coordinatore della struttura di cui al comma 1 spetta:

A. la sottoscrizione degli atti di notifica e di consultazione preventiva al Garante;

B. la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del RGPD.

3. È riservata alla struttura competente in materia di sistemi informativi l'adozione di *policy* in materia di *privacy* e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario. La stessa collabora con la struttura interna prevista al comma 1.

4. La struttura di cui al comma 3 è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di accountability, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al RGPD da parte del RPD.

In particolare:

a. individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente;

b. tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del RPD, come, ad esempio, la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e l'aggiornamento dei disciplinari tecnici trasversali;

c. condivide le evidenze dell'analisi dei rischi con il RPD, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;

d. provvede, ogni qualvolta venga avvertito un problema di sicurezza, nell'ambito delle sue competenze ad attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del RPD;

e. individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del RPD.

Art. 9 Registro dei trattamenti

1. Ai sensi dell'art. 30 RGPD è istituito il Registro unico dei trattamenti, che reca almeno le seguenti informazioni:

a. il nome ed i dati di contatto del Titolare e 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;

h. le categorie di trattamenti effettuati: raccolta, registrazione, organizzazione e strutturazione, conservazione, modifica, estrazione, consultazione, comunicazione, diffusione, interconnessione, archiviazione, limitazione, cancellazione, distruzione.

2. Il registro rappresenta l'elemento centrale per la governance del modello di gestione *privacy* ed è tenuto dal Titolare, in modalità digitale secondo lo schema allegato "*A*", al presente Regolamento, suscettibile di integrazioni che dovessero rendersi necessarie, riportando comunque i dati minimi utili.

3. Ciascun dirigente designato ha comunque la responsabilità di fornire prontamente e correttamente ogni elemento necessario alla regolare tenuta e aggiornamento del Registro.

Art. 10 Valutazioni d'impatto sulla protezione dei dati (DPIA "*Data Protection Impact Assessment*")

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, punti 4 - 6, 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, punto 3, RGPD, 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 le 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 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;

f. ambito geografico dell'attività di trattamento;

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

h. 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 o suo delegato, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

i. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

j. tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

4. 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 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 DPIA.

5. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare di regola affida la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune, che si avvale della collaborazione dei dirigenti designati.

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

7. I dirigenti designati e in particolare il Responsabile della sicurezza dei sistemi informativi e l'ufficio competente per detti sistemi devono assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

8. 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.

9. Il Servizio Sistemi Informativi può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

10. La DPIA non è necessaria nei casi seguenti:

a. se il trattamento non comporta un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, punto 1, RGDP;

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 Privacy prima del maggio 2018 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.

11. 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.

12. 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, 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. 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) devono essere determinati considerando il 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.

13. Il Titolare può raccogliere 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.

14. 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.

15. 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 si intende la violazione della 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 dal Comune.

2. Il responsabile/coordinatore della struttura di cui all'articolo 8 comma 1, nel caso in cui 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 deve avvenire entro 72 ore e comunque senza ingiustificato ritardo. I dirigenti designati e i Responsabili del trattamento sono obbligati ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione. Il RPD supporta il Titolare nella citata notifica, al fine di garantirne la tempestività.

3. 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 sia elevato, 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 rilevata. I rischi per i diritti e le libertà degli interessati possono essere considerati "*elevati*" quando la violazione può, a titolo esemplificativo:

— 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 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il responsabile/coordinatore della struttura di cui all'articolo 8 comma 1 deve opportunamente documentare le violazioni di dati personali rilevate, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intendono 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.

ALLEGATO A

SCHEMA REGISTRO DEI TRATTAMENTI

INFORMAZIONI SUL TRATTAMENTO

N. ordine

Unità organizzative

Descrizione

Finalità oltre ad artt. 822 e 824 CC (demanio pubblico) e D.Lgs 42/2004 (patrimonio culturale nazionale)

Principale base giuridica

Contitolare (eventuale rappresentante)

Principali operazioni di trattamento

Raccolta

Registrazione

Organizzazione e strutturazione

Conservazione

Modifica

Estrazione

Consultazione

Comunicazione

Diffusione

Interconnessione

Archiviazione

Limitazione

Cancellazione

Distruzione

DATI PERSONALI TRATTATI

Categoria

Dati personali particolari ossia Dati sensibili (Si/No)

Termine previsto cancellazione

INTERESSATI AL TRATTAMENTO

Categoria

Consenso (Si/No)

Informativa (Si/No)

DESTINATARI DEI DATI

Categoria

Paesi terzi, organizzazioni internazionali (Si/No)

TRASFERIMENTI

Eventuali Paesi terzi, organizzazioni internazionali

REGISTRO O ARCHIVIO

Digitale (Si/No)

Cartaceo (Si/No)

MISURE DI SICUREZZA

Misure tecniche ed organizzative adottate

ALLEGATO B

GLOSSARIO REGOLAMENTO

Ai fini del presente Regolamento, si intende per:

Titolare del trattamento: l'autorità pubblica (il Comune, e per esso il Sindaco, quale legale rappresentante) che singolarmente o delegando altri determina finalità e mezzi del trattamento di dati personali.

Responsabile del trattamento: il soggetto, pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.

Autorizzato al trattamento: il dipendente della struttura organizzativa del Comune, incaricato dal Responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali).

Responsabile per la protezione dati (RPD): il dipendente della struttura organizzativa del Comune, il professionista privato o impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento.

Registri delle attività di trattamento: elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare del trattamento.

DPIA - Data Protection Impact Assessment - "*Valutazione d'impatto sulla protezione dei dati*": è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

Garante *Privacy*: il Garante per la protezione dei dati personali quale autorità amministrativa pubblica di controllo indipendente.

ALLEGATO C

GLOSSARIO REGISTRI

Ai fini dei registri, si intende per:

Categorie di trattamento

Raccolta, registrazione, organizzazione e strutturazione, conservazione, modifica, estrazione, consultazione, comunicazione, diffusione, interconnessione, archiviazione, limitazione, cancellazione, distruzione, ogni altra operazione applicata a dati personali.

Categorie di dati personali

Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (*username, password, customer* ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale.

Dati inerenti lo stile di vita.

Situazione economica, finanziaria, patrimoniale, fiscale.

Dati di connessione: indirizzo IP, *login*, altro.

Dati di localizzazione: ubicazione, GPS, GSM, altro.

Finalità del trattamento

Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, 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.

Adempimento di un obbligo legale al quale è soggetto il Comune.

Esecuzione di un contratto con i soggetti interessati.

Altre specifiche e diverse finalità.

Misure tecniche ed organizzative

Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.

Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; *firewall*; antintrusione; altro) adottati per il trattamento di cui trattasi ovvero dal Settore/Servizio/Ente nel suo complesso.

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

tecnico - adottati per il trattamento di cui trattasi ovvero dal Settore/Servizio/Ente nel suo complesso.

Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Dati sensibili o particolari

Dati inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale, dati genetici e biometrici, dati relativi a condanne penali.

Categorie interessati

Cittadini residenti; minori di anni 16; elettori; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

Categorie destinatari

Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.

Allegato D

ORGANIGRAMMA