

REGOLAMENTO PRIVACY PER LA PROTEZIONE DEI DATI PERSONALI

**TITOLARE del TRATTAMENTO
COMUNE di ROCCASTRADA**

INDICE:

Art. 1 - Oggetto

Art. 2 - Glossario

Art. 3 - Titolare del trattamento

Art. 4 - Finalità del trattamento

Art. 5 - base giuridica del trattamento - Informative privacy - categorie di dati trattati

Art. 6 - Responsabile del trattamento

Art. 7 soggetti autorizzati al trattamento dati del titolare: autorizzati/incaricati (interni), designati, soggetti esterni all'ente

Art. 8 - Responsabile della protezione dati (DPO/RPD)

Art. 9 – Sicurezza del trattamento - compiti del settore IT (SED) per la Sicurezza del sistema informatico e per il trattamento con i mezzi elettronici

Art.10 Diffusione dati e trasparenza

Art. 11 - Registro delle attività di trattamento

Art. 12 – adozione del DPS e Valutazione d'impatto sulla protezione dei dati (cd DPIA)

Art. 13 - Procedura in caso di violazione dei dati personali (cd. data breach) – quando si deve procedere con la notifica al Garante e agli interessati

Art. 1 Oggetto

Il presente Regolamento ha per oggetto misure procedurali, organizzative 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 "GDPR"), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di _____

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e la normativa vigente in tema di protezione dati personali ad es d.lgs 196/2003 cd Codice Privacy.

Art.2 Glossario

Le definizioni che possono essere rilevanti sono quelle di cui all'**art. 4 del Regolamento Europeo 679/2016 cd GDPR**:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art.3 Titolare del trattamento

1. Il Comune titolare, rappresentato ai fini previsti dal GDPR dal Sindaco pro tempore o da un suo delegato o dal Dirigente di settore o Responsabile P.O. Posizione Organizzativa, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare agisce e vigila che siano rispettati i principi da applicare al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione (salvo le norme in tema di conservazione di atti amministrativi); 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 GDPR.

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 GDPR, 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 (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.

4. Il Titolare adotta misure appropriate per fornire all'interessato l'informativa privacy artt. 13 e ss GDPR anche per ciascun settore quali affissione nei locali dove accede il pubblico e pubblicazione sul sito web.

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 GDPR considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

6. Il Titolare, inoltre, provvede a:

a) nominare il Responsabile della protezione dei dati (DPO o RPD);

b) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

c) nominare designare i Responsabili del trattamento nel

i dirigenti e/o i responsabili di P.O. così come individuati dall'organigramma vigente sono designati e preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza; come per le altre normative che coinvolgono il Comune costoro devono vigilare che nel settore di loro competenza la normativa privacy sia rispettata dagli autorizzati/incaricati.

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 GDPR. 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 GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente 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 GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art.4 Finalità del trattamento

I trattamenti sono compiuti dal Comune 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:

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.

Le principali finalità istituzionali sono ad es:

- le funzioni previste dalle leggi, dallo Statuto, dai regolamenti;
- le funzioni svolte per mezzo di intese, accordi di programma e convenzioni.

Di seguito le principali, ad es.:

1. Finalità di Amministrazione
2. Finalità di Contabilità
3. Finalità di consulenza
4. Finalità connesse all'attività commerciale
5. Finalità di carattere sociale
6. Finalità di informazione, istruzione, cultura e valorizzazione del tempo libero
7. Finalità di amministrazione della popolazione
8. Finalità di carattere elettorale
9. Finalità di attività istituzionali in ambito comunitario e/o internazionale (accordi di collaborazione e gemellaggio)
10. Finalità di ordine e sicurezza pubblica
11. Finalità di protezione civile
12. Finalità di difesa dell'ambiente e della sicurezza della popolazione
13. Finalità di pianificazione urbanistica e amministrazione del territorio
14. Finalità di progettazione, affidamento o esecuzione di opere pubbliche
15. Finalità di accertamento e riscossione di tasse ed imposte
16. Finalità di relazioni con il pubblico

Art.5 base giuridica del trattamento - Informative privacy - categorie di dati trattati

Artt. 6, 9, 10 GDPR, leggi dello Stato e/o regolamenti (quando previsti per legge)

La base giuridica del trattamento dati del Titolare, perseguendo fini istituzionali, è la legge e il rilevante interesse pubblico; talvolta ma in rari casi l'ente ha il consenso quale base giuridica del trattamento; per la propria attività di diritto privato il Titolare ha anche il contratto come base giuridica

PER I DATI PERSONALI "ORDINARI" : la base giuridica è la LEGGE o CONTRATTO: ART. 6 GDPR

PER I DATI (ex) SENSIBILI, BIOMETRICI, GENETICI (di rado) E IN GENERALE QUELLI "PARTICOLARI" la base giuridica è la legge e il rilevante interesse pubblico: si richiama il GDPR considerando 53, 54, art. 9 lett.g), i), j) nonché il dlgs 196/2003 cd.codice privacy art. 2 sexies.

PER I DATI GIUDIZIARI nel significato del GDPR (reati, misure sicurezza, casellario ecc) la base giuridica è solo la legge o regolamento (se previsto dalla legge) oppure l'ordine dell'Autorità Giudiziaria, si veda ad es. GDPR art. 10, d.Lgs n. 51/2018 nonché il d.lgs 196/2003 cd. codice privacy art. 2 octies e 2 sexies let.e),s),aa)

CONSENSO ART. 9 n, 2 LETT. A) GDPR nei casi di trattamento facoltativo di dati particolari basati sul consenso ossia quando non è presente una norma di legge o un rilevante interesse pubblico.

Per quanto riguarda i riferimenti normativi si richiama a mero titolo esemplificativo, la Costituzione, il TUEL testo unico enti locali (d.lgs 267/2000), il codice appalti (dlgs 50/2016) ecc

Si richiamano come se fossero qui trasfuse le informative generali e specifiche per i singoli settori pubblicate anche sul sito web dell'ente, ove sono evidenziati in particolare le tipologie di dati trattati, le finalità e i soggetti anche terzi autorizzati a trattare dati (di norma dipendenti autorizzati e responsabili esterni del trattamento o per obblighi di legge).

Art.6 Responsabile (esterno) del trattamento

Ai sensi dell'art. 28 GDPR il «responsabile del trattamento» è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Oggi il responsabile del trattamento sostituisce quella figura che prima del GDPR si chiamava anche professionista esterno dato che nell'ambito delle proprie attività, **il titolare si può avvalere di soggetti esterni per l'espletamento di alcune attività** e, per il migliore ed efficiente svolgimento della propria attività, nominare altri enti, professionisti o consulenti esterni di fiducia, che sulla base di incarichi o convenzioni stipulate possono trattare dati personali provenienti dal titolare medesimo. Tali soggetti sono autorizzati al trattamento dei dati ai soli fini dell'espletamento dell'incarico ricevuto e nei limiti dello stesso.

Ciò accade ad es nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, quest'ultimo non possa occuparsi personalmente del trattamento e, quindi, assumere le relative funzioni e responsabilità, in quanto si tratta di soggetti autonomi non controllabili da parte titolare del trattamento medesimo che però ha l'onere di vigilare su costoro (ad es relativamente alle misure di sicurezza da adottare nel trattamento di cui si tratta) scegliendo soggetti terzi in possesso, secondo una prudente valutazione, dei requisiti di esperienza, capacità ed affidabilità.

Dopo il GDPR è obbligatoria la nomina contrattuale del responsabile (esterno) del trattamento quanto meno in una clausola del contratto principale e dunque **ciascun settore del Comune titolare dovrà conservare presso la propria sede le nomine di propria competenza da avere a disposizione in caso di controllo**. La nomina, se separata dal contratto principale, è firmata dal dirigente del settore o in ogni caso da chi ha sottoscritto il contratto principale con il responsabile (esterno) del trattamento.

Il sottoscritto Titolare del trattamento non ha ritenuto opportuno nominare alcun responsabile interno del trattamento, che era una figura prevista in via facoltativa dal D.lgs. n. 196/2003 prima del GDPR; tale **figura** è da ritenersi **tacitamente abrogata** con l'entrata in vigore del Reg.Ue 679/2016 cd **GDPR** (che **prevede solo un responsabile esterno e non interno**), infine anche il gruppo di lavoro europeo WPART29 nel parere 1/2010 osserva che il responsabile del trattamento è solo esterno.

Il responsabile deve possedere adeguati requisiti di esperienza, capacità e affidabilità sufficienti per mettere in atto misure tecniche e organizzative adeguate e per svolgere il ruolo di responsabile esterno del trattamento dei dati personali.

Il Responsabile esterno è tenuto a trattare i dati personali nel rispetto dei principi GDPR e attenendosi alle istruzioni del titolare del trattamento, assicurando la riservatezza delle informazioni, dei documenti e degli atti anche amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione, impegnandosi a rispettare rigorosamente tutte le norme relative all'applicazione del D. Lgs. 196/2003 (nella versione attuale) e del GDPR; in particolare il Responsabile esterno si deve impegnare a :

1. trattare i dati nel rispetto dei principi del trattamento dei dati previsti nel regolamento e solo per i fini indicati dal contratto, con divieto di qualsiasi altra diversa utilizzazione;
2. trattare i dati attenendosi alle eventuali istruzioni documentate del Titolare del trattamento dei dati;
3. garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate formalmente alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (il titolare caldeggia che siano fatti sottoscrivere appositi accordi di riservatezza) ; **gli incaricati del responsabile devono essere nominati per iscritto e aver ricevuto la formazione necessaria in materia di protezione dei dati personali prima del trattamento dei dati;**

4. redigere, ai sensi dell'art. 30, p. 2 GDPR, qualora ne ricorrano i presupposti, il registro delle attività di trattamento;
5. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
 - a. la pseudonimizzazione e la cifratura dei dati personali;
 - b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
6. mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente accordo o contratto e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato; il Titolare dell'Amministrazione ha diritto di verificare personalmente le misure di sicurezza adottate in concreto dal responsabile esterno;
7. informare e coinvolgere tempestivamente il Titolare di tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte del Garante privacy;
8. tenendo conto della natura del trattamento, ad assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
9. assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive; inoltre come previsto dagli artt. 33 e ss GDPR in caso di violazione dati – cd **DATA BREACH** - che coinvolga anche quelli del titolare, il responsabile del trattamento **informa** il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione, descrivendo quanto meno
 - 1.- il numero di interessati coinvolti e facilità della loro identificazione,
 - 2.- la tipologia di dati personali violati e dunque se ordinari, particolari (ex sensibili), giudiziari o se sono coinvolti minori;
 - 3.- valutazione dell'impatto della violazione e della gravità delle conseguenze per gli interessati;
 - 4.- se sono stati ripristinati i dati e/o arginati i danni dagli informatici;
 - 5.- durata della violazione;
 - 6.- tutti i parametri necessari per la valutazione del rischio (soprattutto per violazioni informatiche), confrontando anche le ultime raccomandazioni dell' Enisa e linee guide del gruppo di lavoro art.29 in tema di data breach;
 - 7.- dettagliare il danno/evento, le procedure adottate per contenere la violazione e le misure di sicurezza da adottare/adottate al fine di attenuare i possibili effetti negativi e affinché la violazione non si ripeta;
 - 8.- indicare se la violazione mette a rischio i diritti e le libertà degli interessati coinvolti dalla violazione, indicando altresì quale è il livello di rischio dell'evento fra nessun rischio – presenza di rischio – rischio elevato;
10. concordare con il Titolare del trattamento dei dati il testo dell'informativa privacy (da allegare alla nomina) e assistere il Titolare del trattamento al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (artt. 12-22 GDPR).

Il Responsabile esterno del trattamento **non ricorre ad un altro Responsabile se non quando necessario e in ogni caso previa autorizzazione scritta**, anche via pec, del Titolare del trattamento: quando la società intenda avvalersi di un altro responsabile del trattamento (Sub responsabile) per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, è tenuto, pertanto, a richiedere l'autorizzazione alla titolare del trattamento con congruo preavviso.

Nel caso in cui il Responsabile del trattamento (Responsabile primario) ricorra ad un altro Responsabile del trattamento (cd subresponsabile) per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, il primo responsabile dovrà selezionare accuratamente il secondo (e così via in caso di ulteriori subresponsabili, in presenza ad es di appalto di servizi particolarmente estesi) ; su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto per il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento. Nel caso in cui l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento salvo dimostri che l'evento dannoso non gli è imputabile (art. 82 p. 1,3). Il Responsabile esterno del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Art.7 soggetti autorizzati al trattamento dati del titolare: autorizzati/incaricati (interni), designati, soggetti esterni all'ente.

Il trattamento potrà, nel rispetto di quanto previsto dal GDPR 2016/679, avvenire da parte di:

A.- personale del Comune (ad es. dipendenti o collaboratori ecc, con esclusione di chi presta sola mano d'opera e dunque non tratta dati né elettronici né cartacei) appositamente autorizzato/incaricato dal titolare, periodicamente formato anche per la protezione dei dati personali.

L'informativa al dipendente e la nomina di autorizzato/incaricato al trattamento sono atti obbligatori e ai fini di controllo privacy, una volta firmati, entrambi devono essere conservati nel fascicolo di ogni singolo dipendente presso l'Ufficio del Personale.

Ogni dirigente e/o P.O. deve accertarsi che tutto il personale del proprio settore sia formato in materia privacy almeno due volte l'anno e deve acquisire i predetti due atti firmati dal dipendente del settore (ossia l'informativa privacy del dipendente e la nomina quale autorizzato/incaricato del trattamento).

Gli autorizzati/incaricati ora indicati sono tutti coloro che all'interno dell'ente trattano dati in possesso del titolare, limitatamente alle mansioni da svolgere e nel rispetto del contratto di lavoro.

Dopo il GDPR la figura del responsabile interno del trattamento è venuta meno, oggi vi è la possibilità ai sensi dell'art. 29 GDPR (Reg.UE n. 2016/679) e dell'art. 2-quaterdecies del Codice della privacy (D.Lgs. 196 del 2003 come modificato) di nominare espressamente una o più persone fisiche che operano sotto l'autorità del titolare, come designato/i a cui assegnare "specifici compiti e funzioni connessi al trattamento di dati personali".

Quindi per riepilogare è importante avere presente che :

1.-la nomina quale autorizzato/incaricato al trattamento è obbligatoria (sono in generale i dipendenti dell'ente),

2.-la nomina quale designato è facoltativa ed eventuale (sono in generale i dirigenti o le P.O. dell'ente),

3.-la nomina quale responsabile interno del trattamento non è più ammessa,

4.-la nomina quale responsabile esterno del trattamento è obbligatoria e può essere contenuta o nel contratto principale o come separata addenda privacy (ad es per i servizi esternalizzati, vedi paragrafo specifico del presente Regolamento).

B.-i tecnici informatici di fiducia che potranno venire in contatto con i dati nelle operazioni di manutenzione e revisione del sistema informatico hardware e software e predisposizione controllo della copia di back up; I soggetti sopraindicati sono tenuti al rispetto della riservatezza e in gran parte dei casi sono soggetti vincolati al segreto e, in ogni caso, all'adozione di tutte le misure necessarie a garantire il corretto e lecito trattamento e la corretta conservazione dei dati, il tutto in linea con il GDPR;

C.- -terzi in qualità di responsabili esterni del trattamento appositamente individuati quali ad es.:

- professionisti anche sanitari;
- il tecnico informatico che potrà venire in contatto con i dati nelle operazione di manutenzione e revisione del sistema informatico hardware e software e predisposizione controllo della copia di back up; vi è poi
- il gestore del sito web che può visualizzare tutti i dati personali lasciati sul web dall'interessato;
- Al momento non abbiamo un gestore cloud ma se ve ne fosse in futuro l'intenzione, ne sceglieremo uno affidabile e con i server in Paesi UE e che rispetti la normativa privacy di cui al GDPR.
- medico del lavoro, consulenti, revisori, anche al fine di adempiere agli obblighi previsti in ambito fiscale e contabile e in tal caso saranno forniti di norma dati personali comuni. I dati personali ("ordinari") dei cittadini, utenti e fornitori possono essere accessibili al commercialista e il revisore (se nominato) al fine di adempiere agli obblighi previsti in ambito fiscale e contabile. • In caso di fattura elettronica i dati passano attraverso un sistema di Interscambio (SdI), gestito dall'Agenzia delle Entrate visibile direttamente anche dalla Ragioneria dello Stato.

I soggetti sopraindicati sono tenuti al rispetto del medesimo segreto professionale ed all'adozione di tutte le misure necessarie a garantire il corretto e lecito trattamento e la corretta conservazione dei dati, il tutto in linea con il GDPR.

- per i dati degli utenti web si rinvia alla cookie policy del sito web del titolare.
- I dati personali potranno inoltre essere comunicati a titolo esemplificativo ai seguenti soggetti o alle categorie di soggetti terzi sotto indicati: Istituti bancari per la gestione dei pagamenti Istituti bancari per la gestione dei pagamenti; Amministrazioni finanziarie, studi professionali o enti pubblici (ad es ASL, SERT, Comuni, UEPE, altri enti territoriali, autorità giudiziarie ecc) o privati in ogni caso per adempiere ad obblighi normativi; avvocati, società di servizi, studi legali per la tutela dei diritti anche contrattuali.
- Enti incaricati per la riscossione.
- Aggiudicatari di gare di appalto per prestazioni o servizi anche esternalizzati e le società che gestiscono i servizi di gara (ad es tramite MEPA, START).

Per quanto riguarda il pagamento di somme in favore del titolare, sia che Lei utilizzi bollettini o bonifico, in tal caso i dati sono trattati direttamente dalla banca; in ogni caso è possibile che, fornendo i dati bancari, anche solo l'iban, possa emergere dove è il conto corrente, in quale Agenzia ecc, dato che il sistema dei pagamenti bancari è così impostato sulla base di leggi e regolamenti senza che il titolare abbia alcun potere decisionale al riguardo.

In generale i dati personali, oggetto di trattamento per le finalità sopra indicate, non potranno essere comunicati a terzi tranne quando sia necessario o previsto dalla legge come ad es alla Pubblica sicurezza o Autorità giudiziaria o Procura quando sussistono i presupposti di legge i dati personali non verranno diffusi, salvo e nei limiti degli obblighi di trasparenza vigenti e con le eventuali opportune cautele.

- Infine il responsabile della sicurezza e prevenzione (RSPP) quando presente, potrà casualmente venire a conoscenza dei dati durante lo svolgimento dei propri compiti ed è comunque tenuto al segreto professionale.

- potrebbero poi esservi anche nel tempo soggetti terzi appositamente individuati quali ad es. soggetti o società terze che erogano servizi di supporto alle attività della società, ovvero a professionisti con i quali sono stati sottoscritti specifici accordi ai sensi della Normativa o per supporto nella gestione delle attività;

- all'Istat se previsto per legge e in forma aggregata di norma.

Per concludere si vede che i dati personali sono comunicati alle seguenti categorie di soggetti:

- Enti e Pubbliche amministrazioni per adempimenti di legge;

- Società esterne e Professionisti che svolgono servizi per nostro conto in qualità di Responsabili Esterni e legati da impegni contrattuali anche inerenti la privacy.

Art.8 Responsabile della protezione dati (RPD o DPO)

Il Responsabile della protezione dei dati (in seguito indicato con "RPD" o "DPO") è disciplinata dagli artt 37 e ss GDPR ed è una figura completamente diversa dal responsabile del trattamento (art 28 GDPR); la nomina del DPO è divenuta obbligatoria solo in alcune ipotesi individuate dall'art 37 GDPR tra cui, come nel caso del Comune, quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico.

Il titolare deve individuare il DPO in un professionista in possesso di adeguata e comprovata preparazione, stante la particolarità della normativa. L'attuale DPO del Comune Avv Benedetta De Luca con studio in Grosseto, Viale Matteotti 43, è anche in possesso della certificazione UNI 11697:2017 come Responsabile Protezione Dati rilasciata da CEPAS.

Il RPD, nel rispetto di quanto previsto dall'art. 39, par. 1, del RGPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

- a) informare e fornire consulenza al titolare del trattamento nonché agli autorizzati/incaricati del trattamento (ossia i dipendenti) che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;

- b) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento 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;

- d) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;

- d) cooperare con il Garante per la protezione dei dati personali;

- e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed a effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

Per consentire lo svolgimento ottimale dei compiti del DPO il Titolare del trattamento si impegna a:

- 1) mettere a disposizione del RPD (oltre al compenso pattuito) risorse umane al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate (ad es gruppo di lavoro ad hoc);
- 2) garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto con la sua funzione;
- 3) informare il DPO di nuovi trattamenti perché ogni trattamento diverso obbliga a redigere una specifica informativa privacy e se il trattamento è svolto con nuove tecnologie e vi è il rischio di compressione dei diritti privacy degli interessati, il titolare deve redigere una DPIA valutazione impatto rischi, possibilmente assistito dal DPO;
- 4) informare il DPO in caso di violazione dati (cd data breach artt.33 e 34 GDPR) anche per verificare l'eventuale obbligo di notifica al Garante e agli interessati.
- 5) coinvolgere tempestivamente il DPO in tutte le questioni riguardanti la protezione dei dati personali; in particolare :
 - il RPD è invitato a partecipare alle riunioni di coordinamento dei Responsabili P.O. e dei responsabili dei servizi 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, preferibilmente via email;
 - in forza del GDPR 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 lasciare traccia del dissenso del DPO e motivare specificamente la decisione di aver agito diversamente** a quanto indicato dal DPO;
 - accertarsi che il nominativo e i recapiti del DPO siano noti al personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente, anche per rivolgere al DPO eventuali quesiti privacy.**
 - 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.

Art. 9 – Sicurezza del trattamento - compiti del settore IT (SED) per la Sicurezza del sistema informatico e per il trattamento con i mezzi elettronici

Il Comune titolare del trattamento mette 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.

Ex art 32 GDPR 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.

Costituiscono misure tecniche ed organizzative adottate dall'ente: 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.

Si rinvia al DPS e al registro delle attività di trattamento ove sono indicate le misure di sicurezza adottate dall'ente per i mezzi elettronici e non elettronici.

Dato che la maggior parte delle insidie per i dati personali provengono da trattamenti elettronici è essenziale definire i compiti dei tecnici informatici del Comune i quali devono prevedere frequenti controlli periodici per l'aggiornamento, la verifica dell'efficacia e della stabilità delle misure di sicurezza adottate in relazione agli strumenti elettronici utilizzati; in particolare :

- controllare frequentemente l'intero sistema hardware e software oltre che dei sistemi operativi di tutti i mezzi elettronici, verificando altresì l'efficacia e la stabilità delle misure di sicurezza adottate e relative agli strumenti elettronici utilizzati dal titolare del trattamento; controllare in generale il corretto funzionamento di tutti i mezzi elettronici;
- Prendere tutti i provvedimenti necessari per evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back- up;
- predisporre un adeguato sistema di back up (differenziato), assicurandosi della qualità delle copie di back- up dei dati e della loro conservazione e custodia in luogo adatto e sicuro;
- Attivare per tutti i trattamenti effettuati con strumenti elettronici le credenziali di autenticazione assegnate agli incaricati del trattamento e fare in modo che sia prevista la disattivazione dei codici identificativi personali (User- ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo di suddetti codici per oltre tre mesi;
- predisporre un adeguato sistema antintrusione (firewall, antivirus, antispyware, antispamming ecc.) proteggendo gli elaboratori dal rischio di intrusione (violazione del sistema da parte di hackers) e dal rischio di virus mediante programmi e in generale di malware; definire l'attivazione di idonei strumenti per la protezione contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Questi strumenti debbono essere monitorati e aggiornati con la maggior frequenza possibile;
- Proteggere gli elaboratori adottando, nei limiti delle capacità di spesa dell'ente, le misure consigliate dall'Agid e dalle linee guida gli enti del settore; i tecnici informatici dell'ente dovranno redigere da un lato una relazione con la descrizione del sistema elettronico e informatico anche dei singoli settori dall'altro una relazione contenente le misure di sicurezza agid e altre adottate per i mezzi elettronici, entrambe le relazioni dovranno essere dai tecnici medesimi aggiornata periodicamente e inserite come allegati del registro delle attività di trattamento;
- redigere un piano di **disaster recovery** per il ripristino dati ;
- in caso di data breach ossia di violazione dati, dopo essere venuto a conoscenza della violazione, descrivere oltre a tutte le informazioni che riterranno utili anche **1.-** il numero di interessati coinvolti e facilità della loro identificazione, **2.-** la tipologia di dati personali violati e dunque se ordinari, particolari (ex sensibili), giudiziari o se sono coinvolti minori; **3.-** valutazione dell'impatto della violazione e della gravità delle conseguenze per gli interessati; **4.-** se sono stati ripristinati i dati e/o arginati i danni dagli informatici; **5.-** durata della violazione; **6.-** tutti i parametri necessari per la valutazione del rischio (soprattutto per violazioni informatiche), confrontando anche le ultime raccomandazioni dell' Enisa e linee guide del gruppo di lavoro art.29 in tema di data breach; **7.-** dettagliare il danno/evento, le procedure adottate per contenere la violazione e le misure di sicurezza da adottare/adottate al fine di attenuare i possibili effetti negativi e affinché la violazione non si ripeta; **8.-** indicare se la violazione mette a rischio i diritti e

le libertà degli interessati coinvolti dalla violazione, indicando altresì quale è il livello di rischio dell'evento fra nessun rischio – presenza di rischio – rischio elevato

- Consigliare il titolare sulle misure di sicurezza che è opportuno acquisire e informare il Titolare nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza presenti;
- **redigere un decalogo semplice di buone prassi informatiche per gli autorizzati al trattamento non informatici** che indichi come riconoscere i vari malware, comportamenti da evitare, **cosa fare appena ci si accorge di aver subito una violazione informatica in attesa che arrivi l'informatico**, le manovre semplici e urgenti ma importanti per evitare l'ulteriore diffondersi di malware.

Art.10 Diffusione dati e trasparenza – accorgimenti nella pubblicazione

Il Titolare del trattamento è un Comune e dunque un ente soggetto anche a obblighi di trasparenza ai sensi del dlgs 33/2013 e dovere di pubblicazione di atti, alcuni dei quali contenenti dati personali.

Dato che gli obblighi di trasparenza vanno di volta in volta coordinati tra loro e dalla diffusione dei dati consegue che questi sono visibili da un numero indefinito di persone, i dati in concreto pubblicati devono essere **strettamente limitati ai dati che devono essere resi noti** per rispettare l'obiettivo di volta in volta previsto dalle esigenze di trasparenza, avendo cura però di eliminare i dati eccedenti che non possono essere diffusi, evitando ad es la pubblicazione degli allegati all'atto: in presenza di diffusione dati, ancor più se si tratta di dati di minori, il principio di minimizzazione deve trovare la massima applicazione.

In ogni caso nella pubblicazione di alcune tipologie di atti (vedi alcune graduatorie ad es quelle da cui si desume una disabilità o un reddito particolarmente basso tale da ottenere benefici economici ecc), i dati identificativi degli interessati devono essere adeguatamente pseudonominizzati (ad es sostituendo al nominativo il numero di rif. Protocollo e si precisa che sono vietate le iniziali o il codice fiscale).

In generale è vietata la diffusione di dati particolari (art 9 GDPR) e le cautele predette dovranno essere utilizzate ogni qual volta emerga un dato particolare ma **in caso di pubblicazione di un atto, occorre verificare attentamente di volta in volta quali dati dell'interessato possono essere resi visibili.**

Ogni Dirigente e/o P.O. deve vigilare affinché ogniquale volta è prevista la pubblicazione di un atto del settore contenente dati personali, chi procede alla pubblicazione rispetti quanto sopra e che applichi rigorosamente il principio di minimizzazione che vieta la pubblicazione di dati in più (anche se dati ordinari) e che, in alcune tipologie di atti sopraindicate (dove emerge ad es disabilità, disagio economico) utilizzi tutti gli accorgimenti utili per pseudonominizzare tutti gli identificativi della persona (ad es inserendo come unico dato identificativo da pubblicare della persona sia il n. di protocollo).

Art.11 Registro delle attività di trattamento

Il Registro delle attività di trattamento svolte dal Titolare del trattamento costituisce una misura di sicurezza prevista dal GDPR che consente di avere il quadro di insieme dei dati trattati e delle misure di sicurezza presenti ed è stato redatto con le informazioni richieste dall'articolo 30 del GDPR :

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno

comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. il registro deve essere periodicamente aggiornato per questo ogni settore dovrà aggiornare semestralmente la scheda del registro relativa al proprio settore e inviarla alla Segreteria.

3. Il Registro è conservato insieme alla documentazione generale privacy presso l'ufficio delle Segreteria Generale.

Art. 12 – adozione del DPS e Valutazione d'impatto sulla protezione dei dati (cd DPIA)

Il Comune titolare ha deciso di redigere il DPS documento programmatico per la sicurezza che è espressamente definito come una misura di sicurezza in materia di protezione dati personali.

Scopo del documento (DPS) è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate per il trattamento dei dati personali, nonché quello di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

Tali obblighi sono delineati dal D.Lgs. 30 giugno 2003 n. 196 (il Codice in materia di protezione dei dati personali, cd. Codice Privacy) agli articoli 31, 33, 34 e 35 e dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Codice); tale allegato B è stato formalmente abrogato ma ciò non significa che il presente documento costituisce tutt'oggi una utile misura di sicurezza che il titolare ha ritenuto di mantenere, dato che il DPS era previsto per il titolare che tratta dati sensibili o giudiziari con mezzi elettronici.

La struttura del **DPS** inoltre è anche in linea con l'**art. 35 del GDPR** che ha previsto un altro strumento ossia la "Valutazione d'impatto sulla protezione dei dati" (cd DPIA o anche solo PIA): a ben vedere il **DPS** procede ad una mappatura di tutti i dati ed a una valutazione dei rischi su tutti i dati trattati e non solo per quelli in cui la DPIA è obbligatoria, ossia in presenza di un *trattamento che prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.*

In questo caso, 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, n. 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, n. 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'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 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.

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 al Comune.

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 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, 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 RDP 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 GDPR, 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 Privacy prima di procedere al trattamento solo 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. 13 Procedura in caso di violazione dei dati personali (cd. data breach) – quando si deve procedere con la notifica al Garante e agli interessati

Il Comune titolare adotta una procedura precisa per la gestione del data breach ossia in presenza di violazione dei dati, sia elettronici che non elettronici; inoltre in ogni caso di violazioni, anche senza che consegua l'obbligo di notifica al Garante, si tiene traccia della violazione in un registro, conservato con il materiale generale privacy presso la Segreteria Generale del titolare; ogni

settore riceve una scheda con le domande a cui rispondere in caso si verifichi nel settore un data breach. La illegittima gestione di un data breach comporta notevoli sanzioni per il titolare.

Ogni Dirigente e/o P.O. deve vigilare affinché gli incaricati del proprio settore prendano visione della procedura sulla gestione data breach e comprendano le indicazioni da fornire nella predetta scheda del registro.

Si riporta per l'importanza quanto previsto dal GDPR in proposito:

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 dal Comune.

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 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 GDPR, 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 GDPR, 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 GDPR.