COPIA

Deliberazione n. 18
in data 16-01-2021

COMUNE DI PIEVE SANTO STEFANO

PROVINCIA DI AREZZO

Croce di Guerra al Valore Militare

Verbale di Deliberazione della Giunta Comunale

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

L'anno duemilaventuno, addì sedici del mese di gennaio alle ore 11:00 nella Residenza Municipale, convocata con appositi avvisi, la Giunta Comunale si è riunita con la presenza dei Signori:

Marcelli Claudio	**Sindaco**	**Presente**
Mormii Massimo	**Vice Sindaco**	**Presente**
Venturi Chiara	**Assessore**	**Presente**
Gradi Luca	**Assessore**	**Assente**
Cangi Sofia	**Assessore**	**Assente**

Totali presenti n. 3 Totali assenti n. 2

Assiste alla seduta la Dott.ssa Maria Gabriella Bartolucci, Segretario del Comune.

Il Sig. Claudio Marcelli, nella sua qualità di Sindaco, assume la presidenza e riconosciuta legale l'adunanza, dichiara aperta la seduta ed invita i convocati a deliberare sull'oggetto sopra indicato.

COMUNE DI PIEVE SANTO STEFANO

OGGETTO: APPROVAZIONE REGOLAMENTO PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

***

LA GIUNTA MUNICIPALE

PREMESSO che:
- il Regolamento del Parlamento Europeo 679/2016 ha introdotto un nuovo quadro giuridico nella materia della protezione dati personali applicabile dal 25 maggio 2018, ai sensi di quanto disposto dall'articolo 99, paragrafo 2 del Regolamento UE 2016/679;
- la piena applicazione della normativa europea determina la necessità per gli Stati dell'Unione di adeguare la vigente legislazione interna in materia di tutela dati personali, oltre la necessità da parte di tutti i soggetti operatori, pubblici o privati che trattano dati, di ottemperare alle nuove prescrizioni europee;

RICHIAMATA la determinazione n. 324 del 12/10/2020, con cui questo Ente ha affidato il servizio di "Data Protection Officer" (Responsabile della protezione dati) per adeguamento al nuovo Regolamento Europeo n. 679/2016 tramite l'Unione Montana dei Comuni della Valtiberina Toscana di Sansepolcro (AR);

DATO ATTO che l'Ente è altresì tenuto all'adozione del Regolamento per l'attuazione del Regolamento UE 2016/679;

CONSIDERATO che il Regolamento deve stabilire le misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento Europeo (General Data Protection Regulation del 27 aprile 2016 n. 679 indicato come "RGPD" Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche, con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati nell'ambito dell'attività del Comune di Pieve Santo Stefano;

RILEVATO che il Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, si compone di n. 19 articoli e dei seguenti allegati: a) Registro attività e categorie di trattamento, b) Procedura data breach e c) Organigramma privacy;

CONSTATATO che il suddetto Regolamento è archiviato nel sistema di gestione documentale, a disposizione sia del Garante Privacy, sia di chiunque possa vantare un legittimo interesse alla sua consultazione;

RITENUTO meritevole di approvazione in ogni sua parte;

VISTO il parere favorevole, in calce alla presente, espresso dal Segretario Comunale;

CON VOTI UNANIMI;

D E L I B E R A

1. di approvare, per i motivi espressi in premessa ed in ogni sua parte, il Regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, che allegato al presente atto ne forma parte integrante e sostanziale;

2. che il predetto Regolamento si compone di n. 19 articoli e dei seguenti allegati: a) Registro attività e categorie di trattamento, b) Procedura data breach e c) Organigramma privacy;

3. che, con voti unanimi, il presente atto viene dichiarato immediatamente eseguibile.

MGB/pb

VISTO: per il parere favorevole di regolarità tecnica ai sensi dell'articolo
49 del Decreto Legislativo n. 267 del 18/8/2000, come sostituito
dall'articolo 3, comma 1, lettera b) del Decreto Legge n. 174 del 10/10/2012
IL SEGRETARIO COMUNALE
F.to Dott.ssa Maria Gabriella Bartolucci

COMUNE DI PIEVE SANTO STEFANO

Il presente verbale viene letto, approvato e sottoscritto come segue.

IL PRESIDENTE	**IL SEGRETARIO COMUNALE**
F.to Claudio Marcelli	F.to Dott.ssa Maria Gabriella Bartolucci

---

Il sottoscritto Segretario Comunale, visti gli atti d'ufficio,

ATTESTA

⇒ CHE la presente deliberazione:

- ▫ è stata pubblicata all'Albo Pretorio il 23-04-2021 e vi rimarrà per 15 gg. consecutivi, come prescritto dall'articolo 124, del Decreto Legislativo n. 267 del 18/8/2000;
- ▫ è stata comunicata, con lettera n. 4202, in data 23-04-2021 ai signori capigruppo consiliari come prescritto dall'articolo 125, del Decreto Legislativo n. 267 del 18/8/2000;
- ▫ non è soggetta al controllo preventivo;
- ▫ è stata comunicata con lettera n. ..... , in data ..... al signor Prefetto come prescritto dall'articolo 135, del Decreto Legislativo n. 267 del 18/8/2000;
- ▫ è stata trasmessa, con lettera n. ..... , in data ..... al Difensore Civico per il controllo, che ne ha segnato ricevuta il …….. Prot. n. ….. ;

⇒ CHE la presente deliberazione è divenuta esecutiva il 23-04-2021:

- ▫ dalla data di inizio della pubblicazione;
- ▫ decorsi 30 giorni dalla ricezione dell'atto, dei chiarimenti o degli atti integrativi richiesti, senza che il Difensore Civico abbia comunicato il provvedimento di annullamento (articolo 134, del Decreto Legislativo n. 267 del 18/8/2000);
- ▫ avendo il Difensore Civico comunicato di non aver riscontrato vizi di illegittimità;

⇒ CHE la presente deliberazione è stata annullata dal Difensore Civico con decisione n. ..... del ……. .

Lì, 23-04-2021

IL SEGRETARIO COMUNALE
F.to Dott.ssa Maria Gabriella Bartolucci

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

Lì, 23-04-2021

Visto: **IL SINDACO** **IL SEGRETARIO COMUNALE**

Comune di Pieve Santo Stefano (Ar)

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

SOMMARIO

Allegati

Premessa

Il Regolamento europeo ed il Dlgs. n. 101/2018 individuano diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

● il “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;

● il “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;

● i “Soggetti designati”: coloro che, sotto la responsabilità del Titolare del trattamento e nell’ambito del proprio assetto organizzativo, svolgano specifici compiti e funzioni connessi al trattamento di dati personali;

● il “Responsabile della protezione dei dati” (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;

● i “Soggetti autorizzati”: persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Art. 1

Oggetto

Con il presente Regolamento si intendono stabilire le misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell’attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con “RGPD”, Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'ambito dell'attività del Comune di Pieve Santo Stefano .

Art. 2

Titolare del trattamento

Il Comune di Pieve Santo Stefano rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato come “Titolare”).

Il Titolare del trattamento assicura il rispetto dei principi di cui al comma 2 e delle disposizioni del presente Regolamento anche mediante delega delle relative funzioni ai Responsabili dei servizi, secondo le rispettive competenze e responsabilità.

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

Il Titolare mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase

di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. 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.

Il Titolare adotta misure appropriate per fornire all'interessato:

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

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

Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, presenti 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, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento e tenuto conto di quanto indicato dal successivo art. 17.

Il Comune di Pieve Santo Stefano 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.

Qualora la normativa nazionale e regionale, preveda che in talune ipotesi il Comune di Pieve Santo Stefano possa determinare unitamente e congiuntamente ad altri soggetti le finalità e i mezzi del trattamento dei dati, questi si configurano, ai sensi dell'art. 26 Reg. Ue, quali contitolari, con rispettive responsabilità da ripartire e definire in modo trasparente mediante un accordo interno.

Art. 3

Finalità del trattamento

1. I trattamenti sono compiuti dal Comune di Pieve Santo Stefano 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;

- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidati al Comune di Pieve Santo Stefano in base alla vigente legislazione.

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

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

c) l’esecuzione di un contratto con soggetti interessati;

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

Art. 4

Attribuzione di compiti a soggetti designati

1. Con proprio provvedimento, il Titolare del trattamento, nella persona del Sindaco pro-tempore, nomina delle figure di presidio interno (ai sensi dell’art. 2 quaterdecies del Dlgs. 101/2018), di seguito chiamate anche “Soggetti designati attuatori”, da individuarsi in linea di principio nei Responsabili dei singoli servizi che, sotto la sua autorità e responsabilità, svolgano specifici compiti e funzioni connessi al trattamento di dati personali in ottemperanza dei principi dettati in materia di trattamento dei dati personali dall’Art. 5 del Regolamento con funzioni di direzione, coordinamento e vigilanza sugli incaricati sottoposti che, materialmente, procedono ai trattamenti.

In particolare ai Soggetti designati (ovvero “Soggetti designati attuatori”) verranno affidati i seguenti compiti previsti dal Regolamento aventi ad oggetto:

a) la comunicazione delle informazioni nei termini indicati dall’Art. 13 del Regolamento qualora i dati personali siano raccolti presso l’interessato;

b) la comunicazione delle informazioni nei termini indicati dall’Art. 14 del Regolamento qualora i dati personali non siano stati ottenuti presso l’interessato;

c) l’esercizio del diritto di accesso dell’interessato ai sensi dell’Art. 15 del Regolamento;

d) l’esercizio del diritto di rettifica da parte dell’interessato ai sensi dell’Art. 16 del Regolamento;

e) l’esercizio del diritto alla cancellazione da parte dell’interessato ai sensi dell’Art. 17 del Regolamento;

f) l’esercizio del diritto di limitazione del trattamento da parte dell’interessato ai sensi dell’Art. 18 del Regolamento;

g) la notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento ai

sensi dell’Art. 19 del Regolamento;

h) l’esercizio del diritto alla portabilità dei dati ai sensi dell’Art. 20 del Regolamento;

i) l’esercizio del diritto di opposizione ai sensi dell’Art. 21 del Regolamento;

j) l’esercizio del diritto di cui all’Art. 22 del Regolamento;

k) l’adozione, e ove necessario riesame e aggiornamento, delle misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento. Tali misure devono comunque essere adeguate a garantire un livello di sicurezza adeguato al rischio secondo quanto statuito dall’Art. 32 del Regolamento. Fatte salve eventuali misure particolari correlate alle specificità delle finalità del trattamento, le predette misure possono consistere in interventi conformi a linee guida e policy da applicare secondo standard comuni a tutti gli uffici dell’Amministrazione.

l) l'adozione delle misure tecniche e organizzative adeguate ad attuare in modo efficace e fin dalla progettazione i principi di protezione dei dati personali e integrare nel trattamento le garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (privacy by design);

m) l'adozione delle misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento (privacy by default);

n) lo svolgimento degli adempimenti correlati, per quanto di competenza, all'attuazione degli articoli 26 e 28 del Regolamento, concernenti, rispettivamente, gli obblighi correlati alla situazione di contitolarità del trattamento e disciplina del responsabile del trattamento;

o) la formale individuazione, nelle rispettive strutture, degli incaricati del trattamento;

p) la tenuta del registro delle attività di trattamento in modo da assicurarne, per gli aspetti di competenza, la corretta compilazione e il costante aggiornamento e revisione;

q) la rilevazione e la segnalazione al responsabile delle protezione dei dati (DPO), secondo quanto indicato nell'Art. 35 del Regolamento e nelle Linee guida adottate sul tema dal Gruppo di lavoro europeo (WP29), dei casi nei quali effettuare la valutazione d'impatto sulla protezione dei dati personali e lo svolgimento della valutazione di impatto secondo le direttive e previa consultazione del DPO, provvedendo, ove necessario anche alla consultazione preventiva ai sensi dell'Art. 36 del Regolamento.

r) la collaborazione, per quanto di competenza, con il responsabile della protezione dei dati

del Comune di Pieve Santo Stefano, nell'esecuzione dei compiti ad esso attribuiti;

s) la cooperazione, per quanto di competenza, con l'autorità di controllo, nell'esecuzione dei

compiti ad essa attribuiti.

2. Il precedente comma 1 si applica anche in caso di accordo contitolarità di cui al precedente Art. 2, ultimo comma.

Art. 5

Autorizzati al trattamento dei dati

Sono soggetti autorizzati al trattamento i dipendenti e collaboratori che agiscono sotto la diretta autorità del Titolare del trattamento (e supervisione da parte dei "Soggetti designati attuatori"), i quali ai sensi dell'Art. 29 del Regolamento hanno accesso ai dati personali e al loro trattamento previa formale designazione e dopo essere stati debitamente istruiti e formati.

Il precedente comma 1 si applica anche in caso di accordo contitolarità di cui al precedente Art. 3, ultimo comma.

Art. 6

Responsabile della protezione dati

Il responsabile della protezione dei dati del Comune di Pieve Santo Stefano, con le competenze e le prerogative previste dagli articoli 37, 38 e 39 del Regolamento, è un professionista scelto tramite procedura ad evidenza pubblica.

Il DPO è incaricato dei seguenti compiti:

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

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

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

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento.

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

Il Titolare ed il Responsabile del trattamento assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il Titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'Art. 39 del Regolamento fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti

Art. 7

Consenso dell'Interessato

1. Il consenso al trattamento dei dati personali non verrà richiesto agli interessati allorquando il trattamento dei dati venga effettuato dal Comune di Pieve Santo Stefano nello svolgimento dei propri compiti istituzionali di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito dal diritto dell'Unione o dello Stato.

2. Nelle fattispecie diverse da quelle di cui al precedente comma 1, qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

3. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

4. Prima della pubblicazione di dati personali deve essere valutato se le finalità della trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.

5. Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.

6. Per le attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione, anche successivo, del consenso al trattamento.

7. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa modalità con la quale è stato accordato.

8. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Art. 8

Trattamento dei dati particolari

1. Non è consentito trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il divieto di cui al precedente comma non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al comma 1;

b) quando il trattamento è necessario per motivi di rilevante interesse pubblico ai sensi dell'art. 9, par.1, Reg. e secondo quanto dispone l'art. 2-sexies Dlgs. 101/2018.

Art. 9

Trattamento dei Dati Giudiziari

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'Art. 6 paragrafo 1, del RGPD deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato da norma di legge o nei casi previsti dalla legge di regolamento che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

Art. 10

Trattamento di dati personali nei Servizi esternalizzati

Nella ipotesi che a soggetti pubblici o privati esterni siano affidati tramite delega o concessione o contratto lo svolgimento di compiti e/o servizi di competenza del Comune di Pieve Santo Stefano da cui debba conseguire il trattamento di dati personali, il provvedimento o contratto di affidamento deve prevedere norme specifiche attraverso le quali si provvede:

- a nominare il soggetto pubblico o privato ovvero la persona fisica affidataria quale responsabile del trattamento dei dati personali per la durata dell'affidamento;

- ad obbligare il responsabile del trattamento ad osservare le prescrizioni di cui al RGPD e alle altre fonti di diritto dell'Unione e dello Stato in materia di protezione dei dati personali;

- a consentire le verifiche sul rispetto delle predette disposizioni normative.

2. Nelle ipotesi di trattamento dei dati personali di cui al precedente comma, il Soggetto designato del Comune di Pieve Santo Stefano competente per materia in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni.

3. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, é determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.

Art. 11

Comunicazione interna di documenti contenenti dati personali

1. La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera a) del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo ovvero all'interno della struttura organizzativa di questo Ente, per ragioni d'ufficio e nell'ambito delle specifiche competenze dei servizi, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti.

2. Il Soggetto designato attuatore del trattamento può tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione concerna particolari categorie di dati sensibili e/o giudiziari.

Art. 12

Utilizzo di dati da parte dei Componenti degli Organi Politici e di Controllo Interno

1. Il Sindaco, la Giunta, i Consiglieri Comunali, nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti dal Comune di Pieve Santo Stefano nei limiti e con le modalità previsti dalle disposizioni di legge e di regolamenti.

2. Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della segretezza del loro contenuto.

Art. 13

Diritto alla cancellazione - Limitazione

1. Il "diritto all'oblio" attribuisce all'interessato una più ampia tutela e libertà tesa ad ottenere la cancellazione dei propri dati personali. L'interessato ha il diritto ad ottenere la cancellazione dei dati che lo riguardano, senza ingiustificato ritardo, se sussistono uno dei motivi elencati nell'art. 17 del GDPR.

2. Il Titolare e/o il Responsabile del trattamento dell'Ente se ha reso pubblici i dati personali ed è obbligato ai sensi del citato articolo 17 a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli tecniche per inibire la pubblicazione dei dati provvedendo, altresì, ad informare anche i Titolari del trattamento esterni (ai quali i dati personali da trattare sono stati trasmessi) della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici e, in particolare, per garantire l'esercizio di libertà di espressione e di informazione; il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (salute pubblica); quando i dati resi anonimi sono necessari per la ricerca storica o per finalità statistiche o scientifiche; per l'adempimento di un obbligo legale o per la esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Art. 14

Diritto di rettifica e integrazione

1. L'interessato ha il diritto di ottenere la rettifica dei suoi dati personali inesatti nonché, tenuto conto delle finalità del trattamento, l'integrazione dei suoi dati personali incompleti, anche fornendo una dichiarazione integrativa. L'istanza di rettifica o integrazione é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.

2. Alla rettifica ovvero all'integrazione dei dati richiesta dall'interessato provvede, senza ritardo e comunque entro cinque giorni lavorativi dalla data di arrivo della predetta istanza, il Responsabile del procedimento amministrativo cui ineriscono i dati da rettificare o integrare.

3. Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità é data tempestiva comunicazione all'interessato con raccomandata con avviso di ricevimento o con notifica a mani o tramite pec.

4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la rettifica del trattamento

effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 15

Sicurezza del trattamento

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

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono, di norma: 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, altresì, misure tecniche ed organizzative che possono essere adottate dalla struttura cui è preposto ciascun Soggetto designato attuatore in raccordo con la Direzione Gestione Sistemi Informatici e con il Responsabile del Servizio Prevenzione e Protezione per la Sicurezza dell'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.

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

L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

Il Comune di Pieve Santo Stefano e ciascun designato si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune di Pieve Santo Stefano, sezione

Amministrazione trasparente, sottosezione "altri contenuti - dati ulteriori" oltre che nella sezione “privacy” eventualmente già presente.

Art. 16

Registro delle attività e categorie di trattamento

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

a) il nome ed i dati di contatto del Comune di Pieve Santo Stefano, del Sindaco ai sensi del precedente art. 2, eventualmente del Contitolare del trattamento, del DPO;

b) le finalità del trattamento;

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

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

l’eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

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

il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 6.

Il Registro è tenuto dal Titolare, ovvero da uno dei soggetti eventualmente designati ai sensi del precedente Art. 4 presso gli uffici della struttura organizzativa del Comune di Pieve Santo Stefano in forma telematica/cartacea, secondo lo schema allegato A al presente Regolamento.

Il Titolare del trattamento può decidere di affidare al DPO il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

Art. 17

Valutazioni d’impatto sulla protezione dei dati

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.

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’at. 35, pp. 4-6, RGDP.

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

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;

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;

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;

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

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;

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

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;

utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

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.

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 di Pieve Santo Stefano.

Il Titolare deve consultarsi con il DPO 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 DPO 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.

Il DPO 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.

Con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'art. 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'art. 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il Titolare del trattamento è tenuto ad adottare

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:

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);

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;

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;

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.

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.

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.

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. 18

Violazione dei dati personali

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 di Pieve Santo Stefano.

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 soggetto designato attuatore è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

danni fisici, materiali o immateriali alle persone fisiche;

perdita del controllo dei dati personali;

limitazione dei diritti, discriminazione;

furto o usurpazione d'identità;

perdite finanziarie, danno economico o sociale.

decifratura non autorizzata della pseudonimizzazione;

pregiudizio alla reputazione;

perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;

riguardare categorie particolari di dati personali;

comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);

comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

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.

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

Art. 19

Rinvio

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

ALLEGATI

A) Registro attività e categorie di trattamento

B) Procedura data breach

C) Organigramma privacy

ATTIVITA' DI TRATTAMENTO -	logo
IL TITOLARE: Comune di Pieve Santo Stefano	
DATI DEL RESPONSABILE PROTEZIONE DATI: Avv. G. Tofalo	

INFORMAZIONI SUL TRATTAMENTO																			DATI PERSONALI TRATTATI			INTERESSATI AL TRATT.			DESTINATARI DEI DATI	
				Principali operazioni di trattamento																							
Processo/ Macro Attività	Descrizione	Finalità	Principale base giuridica	Raccolta	Registrazione	Organizzazione	Strutturazione	Conservazione	Estrazione	Consultazione	Uso	Comunicazione	Diffusione	Raffronto	Interconnessione	Archiviazione	Limitazione	Cancellazione	Distruzione	Categoria (*)	Dati sensibili (Si/No)	Termine previsto cancell.ne (*)	Categoria (*)	Consenso (Si/No)	Informativa (Si/No)	Categoria (*)	Paesi terzi, org.ni int.li (eventuale) (Si/No)
Risorse Umane / reclutamento personale	Partecipazione bando di concorso sino ad eventuale assunzione (inserire procedura dettagliata)	Adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate e da organi di vigilanza e controllo; Reclutamento del personale con conseguente assunzione e ripartizione funzioni, chiusura procedura concorsuali. Procedimenti concernenti diritti e doveri dei dipendenti (aspettative, permessi studio,permessi legge | RGPD art. 6 e) - D.Lgs.165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", - D.Lgs. 267/2000 "Testo Unico Delle Leggi Sull'ordinamento Degli Enti Locali", - D.P.R. 313/2002- artt. 28 e 32	X	X	X	X	X	X	X	X	X		X	X	X		X		Personali - Identificativi; Personali - Caratteristiche fisiche; Personali - Famiglia; Personali – Istruzione/Cultura; Personali - lavoro; Personali – Giudiziari diversi da condanne penali e reati; Sensibili - Origine razziale/etnica; Giudiziari (condanne penali e reati);	N		Persone fisiche; Cittadini residenti; Cittadini non residenti; altro (cittadini protetti o sottoposti a particolari restrizioni);			x] Istituzioni pubbliche (a titolo esemplificativo: INPS, INAIL, Ministeri, Amministrazione finanziaria, Autorità Giudiziarie, amministrazioni o altri uffici comunali, Agenzie delle Entrate,ANAC); [x] Medici e/o studi medici, in adempimento agli obblighi in materia di igiene e sicurezza del lavoro; [x] Professionisti e/o	No
Risorse Umane / Formazione	(inserire procedura dettagliata)	analisi fabbisogni formativi ed esigenze degli uffici, istruzione e formazione del personale dipendente.	RGPD art. 6 e) - D.Lgs.165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", - D.Lgs. 267/2000 "Testo Unico Delle Leggi Sull'ordinamento Degli Enti Locali", - D.P.R. 313/2002- artt. 28 e 32	X	X	X	X	X	X	X	X	X	X	X	X	X				Personali - Identificativi; Personali - Beni/proprietà/possessi; Personali - Posizione geografica; Personali - Famiglia; Personali – Istruzione/Cultura; Personali – giudiziari diversi da condanne penali e reati; Sensibili - Origine razziale/etnica; Sensibili - Convinzioni religiose/filosofiche;	S		Persone Fisiche; Cittadini residenti; Cittadini non residenti (con eventi di stato civile nel comune);			Organismi pubblici; Soggetti richiedenti (delegati richiedenti certificazioni); Fornitori di servizi; Diffusione (Pubblicazioni matrimonio);	No

Risorse Umane/Gestione trattamento economico dipendenti	(inserire procedura dettagliata)	Predisposizione ed elaborazione cedolini-paga mensile di tutto il personale ; Contabilizzazione e versamento di tutte le trattenute facoltative (prestiti, cessioni, delegazioni di pagamento, assicurazioni, sindacati, partiti politici, | RGPD art. 6 e) - D.Lgs.165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", - D.Lgs. 267/2000 "Testo Unico Delle Leggi Sull'ordinamento Degli Enti Locali"	X	X	X	X	X	X	X	X	X		X	X	X				Personali, Identificativi.	N		Cittadini residenti; Cittadini non residenti;			Organismi Pubblici; Imprese;	No
CONTROLLO ACCESSI	Validazione degli accessi a locali dell'ente	Manutenzione del personale e verifica accessi. Gestione database giuridico e acquisizioni informazione prese presso il dipendente.	RGPD art. 6 c), e) (Regolamento UE 2016/679); D.Lgs n. 196/2003 e provvedimenti garante Privacy	X	X						X									Personali - Identificativi; Sensibili - Biometrici;	S		Dipendenti; Incaricati;			Nessuno;	No
TRASPARENZA – ANTICORRUZIONE	Raccolta, comunicazione o diffusione di documenti, informazioni e dati concernenti l'organizzazione e dell'amministrazione comunale, le attività e le sue modalità di realizzazione. (DL 14/03/2013, n.33) nonché attività di prevenzione della corruzione all'interno	Attività in materia di trasparenza amministrativa e di contrasto della corruzione e della illegalità nell'ente. Diffusione di dati sui beneficiari dei provvedimenti di concessione sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e vantaggi economici di qualunque genere a persone ed enti pubblici e privati.	RGPD art. 6 c) e) - Costituzione; Dlvo n. 33/2013; Dlvo n. 50/2016; Dlvo n. 165/2001; Dlvo n. 82/2005 (CAD); Dlvo n. 50/2016; DPR n. 487/1994; L n. 241/1990; Codice Penale; L n. 109/1992; L n. 190/2012; Dlvo n. 39/2013; Dlvo n. 37/2016; delibera ANAC n. 1310	X	X	X		X	X	X	X	X	X	X		X				Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Immagini/suoni; Personali - Posizione geografica; Personali – Istruzione/Cultura; Personali – Giudiziari, diversi da condanne penali e reati;	N		Dipendenti; Amministratori;			Pubblica Amministrazione; Organismi pubblici; Organi di pubblica sicurezza; Diffusione (atti e provvedimenti con eventuali omissis)	No

Gare di appalto	(inserire procedura dettagliata)	Analisi della situazione economica e dei fabbisogni relativi nel r rispetto dei principi nel rispetto dei principi di economicità, efficacia, tempestività, correttezza, libera concorrenza, non discriminazione, trasparenza, proporzionalità nonché di pubblicità Programmazione gare di appalto e successiva loro pubblicazione.	RGPD art. 6 e) – D.lgs 50/2016	X	X	X		X		X	X	X				X				Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Beni/proprietà/possessi; Personali - Immagini/suoni; Personali - Posizione geografica; Personali – Giudiziari diversi da condanne penali e reati;	S		Cittadini residenti; Imprese; Professionisti; Amministratori;			Organismi pubblici; Organi di pubblica sicurezza;	No
Gestione contabilie e amministrativa contratto di appalto	(inserire procedura dettagliata)	Gestione amministrativa del contratto con il fornitore. Attività finanziaria relativa all'appalto (emissione fatture passive, liquidazione dei pagamenti e registrazione ciclo passivo)	RGPD art. 6 e) – D.lgs 50/2016	X	X	X		X		X	X	X				X				Personali - Identificativi; Personali - Caratteristiche fisiche; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - lavoro; Personali - Comunicazione elettronica Personali - Geolocalizzazione; Personali - Beni/proprietà/possessi; Personali - Immagini/suoni; Personali - Posizione geografica; Personali - Famiglia; Personali – Istruzione/Cultura; Personali – Volontà post-morte; (trapianti); Personali – Giudiziari diversi da condanne penali e reati; Sensibili - Origine razziale/etnica; Sensibili - Opinioni politiche; Sensibili - Convinzioni religiose/filosofiche;	S		Cittadini residenti; Cittadini non residenti; Imprese; Enti; Utenti; Dipendenti; Amministratori; Professionisti; Incaricati;			Pubblica Amministrazione; Organi di pubblica sicurezza;	No

Sicurezza sul Lavoro	(inserire procedura dettagliata)	Attività in materia di tutela della salute e della sicurezza nei luoghi di lavoro. (D.lgs. 09/04/2008 n.81). Predisposizione e aggiornamento DVR, rilascio e verifica	RGPD art. 6 c) e) - D.lgs. n. 81/2008	X	X	X		X	X	X	X	X				X				Personali - Identificativi; Personali - Posizione geografica; Personali - Lavoro; Sensibili - Salute; altro (incidenti o mancati incidenti);	S		Persone Fisiche; Utenti; Dipendenti; altro (fornitori o prestatori opera);			Fornitori di servizi; altro (Datori di lavoro); altro (Medico aziendale); altro (Responsabile Servizio Prevenzione e	No
Protocollo - Comunicazione interna	(inserire procedura dettagliata)	Gestione flussi comunicazione interna.Esame corrispondenza e assegnazione posta, tenuta del registro di protocollo degli archivi e dei sistemi documentali dell'ente nonchè l'archiviazione di atti e documenti nel pubblico interesse.	RGPD art. 6 e) – L. n. 241/1990: DL 82/2005 (CAD); DPR n. 445/200; DPCM 03/12/2013 (regole tecniche protocollo informatico); DPCM 13/11/2014 (regole tecniche documenti informatici); DPCM 22/02/2013 (firme elettroniche); DL n. 42/2004 (codice beni culturali)	X	X	X	X	X	X	X	X	X		X	X	X				Personali - Identificativi; Personali - Caratteristiche fisiche; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Beni/proprietà/possessi; Personali - Immagini/suoni; Personali - Posizione geografica; Personali - Famiglia; Personali – Istruzione/Cultura; Personali – Giudiziari, diversi da condanne penali e reati; Personali – Volontà post-morte; (trapianti); Sensibili - Origine razziale/etnica; Sensibili - Opinioni politiche; Sensibili - Convinzioni religiose/filosofiche;	S		Persone Fisiche;			Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici; Organi di pubblica sicurezza;	No

GESTIONE ECONOMICA	Attività per la gestione economica dell'ente (bilanci, entrate, uscite, retribuzioni, ordini per beni e servizi, fatturazione attiva e passiva ecc..).	Attività di ordina amministrativo contabile quali: trattamento giuridico ed economico del personale (calcolo e pagamento di retribuzioni ed emolumenti vari; applicazione della legislazione previdenziale ed assistenziale; cassa integrazione guadagni), adempimenti di obblighi fiscali o contabili, gestione dei fornitori (amministrazione di contratti, ordini, arrivi, fatture; selezioni in rapporto alle necessità), gestione contabile o di tesoreria (amministrazione della contabilità individuale e	RGPD art. 6 b), e) - D.Lgs. n. 267/2000; regolamenti comunali.	X	X	X	X	X	X	X	X	X	X	X	X	X				Personali - Identificativi; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Beni/proprietà/possessi; Personali - Famiglia; Personali – Istruzione/Cultura; Sensibili - Appartenenza sindacale;	S		Persone Fisiche; Imprese; Enti; Utenti; Dipendenti; Amministratori; Professionisti; Incaricati;			Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici; altro (Tesoreria Comunale); altro (Servizi di accertamento e riscossione); Diffusione (Pubblicazione provvedimenti con eventuali omissis)	No
GESTIONE TERZI	Gestione altri soggetti (incarichi professionisti, OIV, incarichi legali, prestazioni occasionali ecc…).	Affidamenti a terzi di incarichi per coprire esigenze alle quali non è possibile far fronte con personale interno.	RGPD art. 6 e) - DLgs n. 267/2000 (T.U.EE.LL.); DLgs n. 165/2001; DLgs n. 50/2016	X	X	X		X		X	X	X	X			X				Personali - Identificativi; Personali - Comunicazione elettronica; Personali - Lavoro; Personali - Posizione geografica; Personali –	N		Persone Fisiche; Imprese; Professionisti; Incaricati; Rappresentanti;			Fornitori di servizi; Società appaltatrici; Banche; Diffusione (atti e provvedimenti con eventuali omissis)	No
PROTEZIONE CIVILE	Interventi di protezione civile (in emergenza, di coordinamento volontari ecc…).	Svolgimento di attività nel pubblico interesse ed in situazioni di emergenza (previsione e prevenzione dei rischi, soccorso alla popolazione colpite, contrasto e superamento dell'emergenza, e mitigazione del rischio).	RGPD art. 6 e) - L n. 225/1992	X	X	X		X		X	X	X				X				Personali - Identificativi; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Beni/proprietà/possessi; Personali - Posizione geografica; Personali - Famiglia;	S		Persone Fisiche; altro (Volontari);			Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici; Organi di pubblica sicurezza; altro (Associazioni di volontariato);	No

Polizia Municipale	(inserire procedura dettagliata)	Programmazione, preparazione svolgimento attività ispettive su pratiche edilizie, raccolta segnalazioni, controllo DIA e SCIA. Attività sanzionatoria con conseguente avvio del relativo procedimento. Adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate	RGPD art. 6 e) – Codice Civile, Penale, Normativa varia nazionale regionale e comunitaria, regolamenti comunali.	X	X	X		X		X	X	X				X				Personali - Identificativi; Personali - Situazione economica; Personali - lavoro; Personali - Comunicazione elettronica Personali - Geolocalizzazione; Personali - Beni/proprietà/possessi; Personali - Immagini Personali - Posizione geografica; Personali - Famiglia; Personali – Giudiziari diversi da condanne penali e reati;	S		Cittadini residenti; Cittadini non residenti; Imprese; Enti; Utenti; Dipendenti; Amministratori; Professionisti; Incaricati;	Pubblica Amministrazione;	N	Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici; Organi di pubblica sicurezza;	No
Barrier	Domanda di Accesso ai contributi	Ricezione istanza, avvio procedimento, controllo richiesta e requisiti conclusione pratica		X	X	X		X		X	X	X				X							Cittadini residenti; Cittadini non residenti; Imprese;					
SERVIZI A DOMANDA INDIVIDUA	Attività socio assistenziali e legate ai servizi a domanda individuale (individuate	Attività di pubblico interesse gestite direttamente dal Comune e di cui non vi è un obbligo istituzionale che non sono state dichiarate gratuite per legge	GDPR art. 6 e) – L. n. 131/1983; DM 31/12/1983 (categorie dei servizi a domanda individuale)	X	X	X	X	X		X	X	X				X				Personali - Identificativi; Personali - Situazione economica; Personali - Famiglia; Personali – Istruzione/Cultura;	N		Cittadini residenti;			Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici;	N
SOCIALE - SOSTEGNO ECONOMICO	Attività legate alla concessione di benefici economici. (sostegno della maternità, locazione o situazioni di emergenza abitativa, concessioni di	Tenuta, aggiornamento, comunicazione e diffusione dell'albo beneficiari dei contributi economici erogabili. La pubblicazione viene effettuata tramite albo pretorio presente in sede comunale tramite un protocollo riservato e conseguente attivazione della pratica in caso di richiesta del beneficiario.	GDPR art. 6 e) – Costituzione; DPR n. 616/1977; Codice Civile; L n. 42/1990L n. 241/1990; DL n. 109/1998 e successive modifiche da parte del DPR 159/2013 ; L n. 448/98; normativa regionale e	X	X	X		X	X	X	X	X	X	X		X	X			Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Beni/proprietà/possessi; Personali - Famiglia; Personali –	S		Cittadini residenti;			Pubblica Amministrazione; Organismi pubblici;	N

SOCIALE - LAVORO	Attività in materia di occupazione e lavoro. La coop. è a conoscenza dei dati personali e particolari degli utenti aventi disagi economici e familiari o	Adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate o esecuzione di compiti nell'interesse pubblico. In particolare: attività di carattere sociale relative all'incontro domanda/offerta di	GDPR art. 6 e) – Costituzione; legge 68/1999, normativa ed indicazioni regionali	X	X	X		X		X	X	X		X	X				Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Posizione geografica;	S		Persone Fisiche; Imprese; Enti; Utenti;			Pubblica Amministrazione; altro (potenziali datori di lavoro);	N
SOCIALE – DOMICILIARI	L'assistenza domiciliare sarà affidata ad una ditta esterna (soggetto ancora in fase di definizione) a cui viene affidato il servizio. La responsabile ufficio sociale passa una scheda personale con le info necessarie (condizione sociale,sanitaria del soggetto..) al referente della ditta esterna, dopo di che	Interventi di interesse pubblico mirati ad offrire servizi socio assistenziali o sanitari, anche tramite altre strutture pubbliche o private, a cittadini non autosufficienti o in condizioni di fragilità.	GDPR art. 6 e) – L n. 328/2000; DPCM 14 Febbraio 2001																Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Posizione geografica; Personali – Giudiziari, diversi da condanne penali e reati; Personali - Famiglia; Personali – Istruzione/Cultura; Sensibili - Salute;	S		Cittadini residenti; altro (soggetti in particolari condizioni di disagio);			Pubblica Amministrazione; Organismi pubblici;	N

SOCIALE - MINORI E MONITORAGGIO FAMILIARE	Politiche Sociali - Attività di monitoraggio di famiglie con minori richesta da Procura e prefettura. Attività di Monitoraggio tecnico interventi in ambito sociale e sociosanitario.	Interventi di interesse pubblico mirati ad offrire servizi socio assistenziali o sanitari, anche tramite altre strutture pubbliche o private, a minori e relativi nuclei familiari in condizioni di fragilità. Interventi di interesse pubblico mirati ad offrire servizi socio assistenziali o sanitari in materia di programmazione partecipata delle attività e dei servizi sociali.	GDPR art. 6 e) – Codice Civile; L n. 176/1991 (ratifica convenzione internazionale di New York); L n. 184/1983; normativa regionale. L. n. 328/2000: LR n. 1/2004; DL n. 117/2017																Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Posizione geografica; Personali – Giudiziari, diversi da condanne penali e reati; Personali - Famiglia;	S		altro (Minori e loro famigliari); ttadini residenti; altro (soggetti in particolari condizioni di disagio);		Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici;	N
SOCIALE - SERVIZI DI TRASPORTO E SERVIZI DI TRASPORTO MINORI CON 104	Politiche Sociali - Attività di monitoraggio di famiglie con minori richesta da Procura e prefettura. Attività di Monitoraggio tecnico interventi in ambito sociale e sociosanitario.	Interventi di interesse pubblico mirati ad offrire servizi socio assistenziali o sanitari, anche tramite altre strutture pubbliche o private.	GDPR art. 6 e) – Varia normativa in ambito socio-assistenziale	X	X	X	X	X	X	X	X	X		X	X	X				Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Posizione geografica; Personali – Giudiziari, diversi da condanne penali e reati; Personali - Famiglia;	S		Cittadini residenti; altro (soggetti in particolari condizioni di disagio);		Pubblica Amministrazione; Organismi pubblici;	N

SOCIALE - CONTRIBUTI	In seguto a bando viene stilata una graduatoria in base a punteggi decisi dal bando. Invio di comunicazione all'utente a cui la domanda viene accettata 1 ad 1 con numero di protocollo e graduatoria pubblicata con numero di protocollo	Interventi di interesse pubblico mirati ad offrire servizi socio assistenziali o sanitari, anche tramite altre strutture pubbliche o private, relative a misure di protezione giuridica per aiutare persone con limiate capacità di autonomia.	GDPR art. 6 e) – Codice Civile, L n. 6/2004	X	X			X		X	X	X				X				Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Beni/proprietà/possessi; Personali - Posizione geografica; Personali - Famiglia; Personali – Istruzione/Cultura; Personali – Giudiziari, diversi da condanne penali e reati;	S		Cittadini residenti; altro (cittadini protetti o sottoposti a particolari restrizioni);			Organismi pubblici; Organi di pubblica sicurezza;	N
SOCIALE - SERVIZI PER I GIOVANI	Gestione di progetti per inserimenti lavorativi dei giovani;	Attività svolte nel pubblico interesse con riferimento all'area territoriale del Centro per l'Impiego in materie di: consulenza, orientamento, comunicazione, circolazione ed elaborazione delle informazioni su alcune specifiche tematiche (lavoro, ecc..) e di progettazione condivisa con altri soggetti di soluzioni per la	GDPR art. 6 e) -	X	X	X		X		X	X	X				X				Personali - Identificativi; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Posizione geografica; Personali – Istruzione/Cultura; Sensibili - Salute;	S		Cittadini residenti; altro (soggetti in particolari condizioni di disagio);			Imprese; Enti; Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici; Organi di pubblica sicurezza;	N
SOCIALE – AGEVOLAZIONI TRIBUTARIE	Agevolazioni, esenzioni tributarie o tariffarie ai fini dei servizi di natura sociale o scolastica	Interventi di interesse pubblico a carattere sociale per particolari categorie di cittadini inerenti la riduzione delle imposte comunali o la riduzione di tariffe per l'accesso ai servizi educativi e sociali.	GDPR art. 6 e) – L n. 328/2000	X	X	X	X	X		X	X	X		X		X				Personali - Identificativi; Personali - Beni/proprietà/possessi; Personali - Situazione economica; Personali - Posizione geografica; Sensibili -	S		Persone Fisiche;			Organismi pubblici; altro (Concessionari riscossione tributi);	N

GESTIONE PERSONALE	Gestione dipendenti e altri soggetti impiegati a vario titolo presso l'ente (malattie, pratiche previdenziali, deleghe sindacali, maternità, permessi ecc..) di dipendenti all'attivo	Adempimenti in relazione al trattamento giuridico ed economico del personale (rilevazione presenze; applicazione della legislazione previdenziale ed assistenziale ecc..), reclutamento, selezione, valutazione e monitoraggio, formazione professionale.	GDPR art. 6 e) – Contratti di lavoro e normativa varia.	X	X	X	X	X	X	X	X	X	X	X	X	X				Personali - Identificativi; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Posizione geografica; Personali - Famiglia; Personali – Istruzione/Cultura; Sensibili - Opinioni politiche; Sensibili - Convinzioni	S		Persone Fisiche; Dipendenti;			Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici; altro (Tesoreria Comunale); altro (Servizi di accertamento e riscossione); altro (Medico Aziendale); altro (Responsabile Servizio Prevenzione e Protezione); altro	N
SICUREZZA SUL LAVORO - PREVENZIONE E PROT	Attività in materia di tutela della salute e della sicurezza nei luoghi di lavoro. (D.lgs. 09/04/2008 n.81).	Adempimenti normativi obbligatori in materia di tutela della salute e della sicurezza nei luoghi di lavoro.	GDPR art. 6 c) e) - D.lgs. n. 81/2008	X	X	X		X	X	X	X	X				X				Personali - Identificativi; Personali - Posizione geografica; Personali - Lavoro; Sensibili - Salute; altro (incidenti o mancati incidenti);	S		Persone Fisiche; Utenti; Dipendenti; altro (fornitori o prestatori opera);			Fornitori di servizi; ; altro (Datori di lavoro); altro (Medico aziendale); altro (Responsabile Servizio Prevenzione e Protezione);	N
RAGIONERIA e CONTABILITA'	Gestione economico-finanziaria dell'Ente, fatturazione elettronica, rendicontazione e fatture clienti e fornitori, controllo economico	Predisposizione ed elaborazione cedolini-paga mensile di tutto il personale ; Contabilizzazione e versamento di tutte le trattenute facoltative (prestiti, cessioni, delegazioni di pagamento, assicurazioni, sindacati, partiti politici, pignoramenti, etc.) ; Gestione pignoramenti presso terzi (dichiarazione	RGPD art. 6 e) - D.Lgs.165/2001 aggiornato al D.Lgs 75/2017 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", - D.Lgs. 267/2000 ed ulteriori modifiche "Testo Unico Delle Leggi Sull'ordinamento Degli Enti Locali",	X	X	X	X	X	X	X	X	X		X	X	X				Personali, Identificativi.	N		Cittadini residenti; Cittadini non residenti;			Organismi Pubblici; Imprese;	No

SISTEMA INFORMATICO	Gestione del silema informatico comunale. Gestione degli utenti e degli accessi alle risorse e relativa profilazione, acquisizione, installazione e mantenimento delle risorse nonché erogazione di servizi	Esecuzione di compiti nell'interesse pubblico per la gestione del sistema informativo dell'ente (sistemi di salvataggio e ripristino, sicurezza, utenti e accessi alle risorse, progettazione, acquisizione, installazione e mantenimento, amministrazione di fornitori, contratti, ordini, consegne, fatture) compresa gestione dei sistemi di posta	GDPR art. 6 e) -; provvedimenti garante Privacy (Internet, Amministratori di sistema); Circolare AgID n. 2/2017 (sicurezza)	X	X	X	X	X	X	X	X	X		X	X					Personali - Identificativi; Personali - Lavoro; Personali – Istruzione/Cultura; altro (log di navigazione internet);	N	max 1	Dipendenti; Incaricati;			Fornitori di servizi; (su richiesta); altro (RPD dell'ente);	N
SITO WEB ISTITUZIONALE	Attività mirata allo sviluppo di progetti finanziabili da altri soggetti pubblici o privati.	Svolgimento di attività per la ricerca di finanziamenti in ambito nazionale ed europeo da utilizzarsi per il raggiungimento di obiettivi e la realizzazione di progetti di pubblico interesse.	GDPR art. 6 e)	X	X	X		X	X	X	X	X	X			X				Personali - Identificativi; Personali - Comunicazione elettronica; Personali - Posizione geografica; Personali – Istruzione/Cultura;	N		Dipendenti; Amministratori; Incaricati; Rappresentanti ; altro: (membri di associazioni);			Pubblica Amministrazione; Organismi pubblici; Diffusione (atti e provvedimenti con eventuali omissis)	N
TRASPARENZA – ANTICORRUZIONE	Raccolta, comunicazione o diffusione di documenti, informazioni e dati concernenti l'organizzazione e dell'amministrazione comunale, le attività e le sue modalità di realizzazione. (DL 14/03/2013, n.33) nonché attività di prevenzione della corruzione all'interno dell'ente. Diffusione di	Adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate e da organi di vigilanza e controllo; in particolare attività in materia di trasparenza amministrativa e di contrasto della corruzione e della illegalità nell'ente. Diffusione di dati sui beneficiari dei provvedimenti di concessione sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e vantaggi economici di qualunque genere a persone ed enti pubblici	GDPR art. 6 c) e) - Costituzione; Dlvo n. 33/2013; Dlvo n. 50/2016; Dlvo n. 165/2001; Dlvo n. 82/2005 (CAD); Dlvo n. 50/2016; DPR n. 487/1994; L n. 241/1990; Codice Penale; L n. 109/1992; L n. 190/2012; Dlvo n. 39/2013; Dlvo n. 37/2016; delibera ANAC n. 1310	X	X	X		X	X	X	X	X	X	X		X				Personali - Identificativi; Personali - Abitudini/stile vita/comportamento; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Immagini/suoni; Personali - Posizione geografica; Personali – Istruzione/Cultura; Personali – Giudiziari, diversi da condanne penali e reati;	N		Dipendenti; Amministratori;			Pubblica Amministrazione; Organismi pubblici; ; Organi di pubblica sicurezza; Diffusione (atti e provvedimenti con eventuali omissis)	N

PRIVACY	Attività legate all'applicazione della normativa in materia di protezione dei dati personali.	Adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate o esecuzione di compiti nell'interesse pubblico. In particolare in materia di protezione delle persone	GDPR art. 6 c), e) (Regolamento UE 2016/679); D.Lgs n. 196/2003 e provvedimenti garante Privacy	X	X	X	X	X	X	X	X	X	X	X	X	X	X				Personali - Identificativi; Personali - Lavoro; Personali - Comunicazione elettronica; Personali – Istruzione/Cultura; Personali – Giudiziari, diversi da condanne penali e reati;	N		Persone Fisiche; Utenti; Dipendenti; Amministratori; Professionisti; Incaricati;			Pubblica Amministrazione; Organismi pubblici; ; altro (RPD dell'ente); Diffusione (soli dati RPD dell'ente);	N
GESTIONE PERSONALE	Gestione dipendenti e altri soggetti impiegati a vario titolo presso l'ente (malattie, pratiche previdenziali, deleghe sindacali, maternità, permessi ecc..) di dipendenti all'attivo	Adempimenti in relazione al trattamento giuridico ed economico del personale (rilevazione presenze; applicazione della legislazione previdenziale ed assistenziale ecc..), reclutamento, selezione, valutazione e monitoraggio, formazione professionale.	GDPR art. 6 e) – Contratti di lavoro e normativa varia.	X	X	X	X	X	X	X	X	X	X	X	X	X	X				Personali - Identificativi; Personali - Situazione economica; Personali - Lavoro; Personali - Comunicazione elettronica; Personali - Posizione geografica; Personali - Famiglia; Personali – Istruzione/Cultura; Sensibili - Opinioni politiche; Sensibili - Convinzioni religiose/filosofiche; Sensibili - Appartenenza sindacale; Sensibili - Salute;	S		Persone Fisiche; Dipendenti;			Fornitori di servizi; Pubblica Amministrazione; Organismi pubblici; altro (Tesoreria Comunale); altro (Servizi di accertamento e riscossione); altro (Medico Aziendale); altro (Responsabile Servizio Prevenzione e Protezione); altro (Rappresentanti dei lavoratori sulla sicurezza); altro (Organismi sindacali); altro (Organismi paritetici in materia	N

Data Breach Policy

Procedura di notifica di violazione dei dati personali

INDICE

1. PREMESSA

Il Comune di Pieve Santo Stefano ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Ente e per poter comunicare nei tempi e nei modi previsti dalla normativa europea all'Autorità Garante e/o agli interessati.

2. SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni di dati personali trattati dal **Comune di Pieve Santo Stefano** in qualità di Titolare del trattamento (di seguito "Titolare del trattamento").

3. COS'E UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

1. Divulgazione di dati personali a soggetti non autorizzati;
2. Perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
3. Perdita o furto di documenti cartacei;
4. Infedeltà aziendale (ad esempio: *data breach* causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
5. Accesso abusivo (ad esempio: *data breach* causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
6. Casi di pirateria informatica (usurpazione delle credenziali di accesso - fishing);
7. Banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "*owner*";
8. Virus o altri attacchi al sistema informatico o alla rete aziendale;
9. Violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);
10. Smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
11. Invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

4. A CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

a. I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;

b. qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

5. A QUALI TIPI DI DATI SI RIFERISCE QUESTA PROCEDURA

Queste procedure si riferiscono a:

- Dati personali trattati “da” e “per conto” del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;

- Dati personali conservati o trattati a mezzo di qualsiasi altro Sistema in uso nell’Ente.

Per «dato personale» si intende: 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.

6. GESTIONE COMUNICAZIONE DI DATA BREACHES

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un Capo area sotto la supervisione del RPD.

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il Capo Area il quale si occuperà, senza ritardo con il supporto dei Destinatari stessi, di informare il Titolare del trattamento mediante la compilazione della scheda "Raccolta informazioni Violazione dati".

7. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque passaggi, di cui due eventuali:

Step 1: Identificazione e indagine preliminare;

Step 2: Contenimento, recovery e *risk assessment*;

Step 3: Notifica all'Autorità Garante (eventuale);

Step 4: Comunicazione agli interessati (eventuale);

Step 5: Documentazione della violazione.

Step 1: Identificazione e indagine preliminare

La Sezione "Raccolta informazione Violazione dati "debitamente compilata, permetterà al Titolare del trattamento o un Capo Area di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di *Data Breach* (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il *risk assessment* (step 2).

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o il capo area del settore interessato dovrà coinvolgere in tutta la procedura indicata nel presente documento anche l'amministratore di sistema

Detta valutazione iniziale sarà effettuata attraverso l'esame delle

informazioni riportate nella sezione "Raccolta informazioni violazione dati", quali:

- la data di scoperta della violazione (tempestività);

- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- la descrizione delle conseguenze dell'incidente
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- le banche dati o archivi anche cartacei violati
- la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un *Data Breach* è avvenuto, il Titolare del trattamento e l'amministratore di sistema dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento valuterà la gravità della violazione utilizzando l'allegato A - Modulo di valutazione del Rischio connesso al *Data Breach* che dovrà essere esaminato unitamente alla scheda "raccolta informazioni Violazione dati", tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR .

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Notifica all'Autorità Garante competente (eventuale)

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, **il Comune di Pieve Santo Stefano**

provvederà, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Pertanto, il Titolare del trattamento individuerà la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Step 4: Comunicazione agli interessati (eventuale)

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, sulla base della procedura di cui allo *step* 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, **il Comune di Pieve Santo Stefano** dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento o il capo area dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (RPD); (eventuale)
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o il capo area dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e- mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di *Data Breach,* ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A, **il Comune di Pieve Santo Stefano** sarà tenuto a documentarlo.

Tale documentazione sarà affidata al Titolare del trattamento o all'amministratore di Sistema (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta del Registro dei *Data Breach*, secondo le informazioni ivi riportate.

Il Registro dei *Data Breach* deve essere continuamente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi.

A – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL *DATA BREACH*

***Assessment* di gravità**	**A cura del RPD insieme con ASICT (se del caso) e il Responsabile dell'ufficio coinvolto della violazione**
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori aziendali: operation, research, financial, legal, liability o ALLEGATO r reputation?	
Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti:	

a.Dati personali generici	
b. I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: ▪ origine razziale o etnica; ▪ opinion politiche, convinzioni religiose o filosofiche; ▪ appartenenza sindacale; ▪ dati genetici; ▪ dati biometrici; ▪ dati giudiziari; ▪ relative alla salute all'orientamento sessuale di una persona.	
c. Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);	
d. Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori);	
e. Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;	
Altro:	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati	

dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione (1, 2 o 3) e motivazioni:	

Notificazione del Data Breach all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach agli interessati	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del Data Breach ad altri soggetti	Si/NO Se sì, notificato in data: Dettagli:

Dpo Centro Studi Enti Locali Spa

Avv Giuseppina Tofalo