COMUNE DI JESOLO

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO E DEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" COME MODIFICATO DAL DECRETO LEGISLATIVO 10 AGOSTO 2018, N. 101.

Approvato con delibera di consiglio comunale n. 123 del 30/11/2021

ARTICOLO 1
AMBITO DI APPLICAZIONE

1. Il presente Regolamento, adottato in attuazione del Regolamento (UE) 27 aprile 2016, n. 679 (di seguito Regolamento UE) e del D. Lgs. n. 196/2003 come novellato dal D. Lgs. n. 101/2018 (di seguito Codice in materia di protezione dei dati personali), disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi all'interno del Comune.
2. Il Comune considera il trattamento lecito, corretto e trasparente dei dati personali una azione prioritaria al fine di instaurare e mantenere un rapporto di fiducia con il personale e i terzi interessati e a tal fine ritiene prioritario introdurre metodologie e prassi operative specifiche per l'adeguamento alle prescrizioni del GDPR, tenendo conto del contesto specifico del Comune di Jesolo.
3. Allo stesso tempo il Comune ritiene importante disporre procedure atte a verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative adottate e a dimostrare che il Comune di Jesolo è conforme ai requisiti di sicurezza previsti dall'art. 32 del GDPR e conforme a riconosciuti standard di sicurezza a livello internazionale.
4. A tal fine tutti coloro che trattano dati personali all'interno del Comune perché espressamente autorizzati o per l'espletamento di compiti propri della struttura cui funzionalmente afferiscono, dovranno effettuare il trattamento secondo la politica di protezione dei dati personali stabilita dal presente Regolamento.

ARTICOLO 2
DEFINIZIONI

1. trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, 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;
2. dato personale: qualunque informazione riguardante una persona fisica identificata o identificabile; 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;
3. categorie particolari di dati: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale;
4. dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
5. 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;
6. 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;
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 Europea o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto

dell'Unione Europea o degli Stati membri;

8. responsabile esterno: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9. delegato interno: il soggetto appositamente delegato, responsabile dell'attuazione del presente Regolamento all'interno delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono. Ove non siano nominati dei Delegati interni, le funzioni loro attribuite dal presente Regolamento vengono svolte dal Sindaco. All'interno del Comune i delegati interni sono individuati da appositi atti di nomina;
10. responsabile della transizione al digitale: figura i cui compiti sono definiti dall'art. 17, comma 1-sexies del Codice dell'Amministrazione Digitale (emanato con D.lgs. n.82 del 7 marzo 2005, quale risultante dalle successive modifiche e integrazioni, inclusa l'ultima disposizione integrativa e correttiva di cui al decreto legislativo 13 dicembre 2017, n. 217);
11. responsabile della conservazione dei documenti informatici: figura i cui compiti sono definiti dall'art. 44 del Codice dell'Amministrazione Digitale (emanato con D.lgs. n.82 del 7 marzo 2005, quale risultante dalle successive modifiche e integrazioni, inclusa l'ultima disposizione integrativa e correttiva di cui al decreto legislativo 13 dicembre 2017, n. 217);
12. incaricati al trattamento: le persone fisiche formalmente autorizzate e istruite a trattare i dati personali sotto l'autorità diretta del Titolare e/o del Delegato interno e per le finalità stabilite dal Titolare (artt. 4, 29, 32, 39 del regolamento UE);
13. interessato al trattamento: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
14. 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;
15. terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare o il contitolare del trattamento, il responsabile esterno del trattamento, il delegato interno del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
16. destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi;
17. 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;
18. 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;
19. limitazione di trattamento: il vincolo apposto a dati personali, conservati con l'obiettivo di limitarne il trattamento in futuro;
20. 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 o che sia gestito attraverso strumenti manuali o automatizzati;
21. responsabile per la protezione dei dati: figura specializzata nel supporto al Titolare del trattamento prevista dall'art. 37 e ss. del regolamento UE;
22. registro attività di trattamento: elenco, in forma cartacea o digitale, delle attività di trattamento dei dati personali effettuate sotto la propria responsabilità dal Titolare e dal Responsabile esterno per la protezione secondo le rispettive competenze;
23. valutazione d'impatto sulla protezione dei dati: procedura atta a descrivere il trattamento, valutarne le necessità e

proporzionalità e a garantire la gestione dei rischi dei diritti e delle libertà delle persone fisiche legate al trattamento dei loro dati personali.

24. 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;

25. rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta per quanto riguarda gli obblighi rispettivi ai sensi del Regolamento UE sulla protezione dei dati personali;

26. 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;

27. gruppo imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

28. 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;

29. autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE : per l'Italia il Garante per la protezione dei dati personali;

30. trattamento transfrontaliero: 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 Europea, ma che incide o può incidere in modo sostanziale su interessati in più di uno Stato membro;

31. autorità di controllo interessata: un'autorità di controllo interessata al trattamento di dati personali in quanto:

a) il titolare 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 possono essere influenzati in modo sostanziale dal trattamento; oppure

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

32. 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.

ARTICOLO 3
PRINCIPI

1. Il trattamento dei dati personali viene effettuato dal Comune in applicazione dei principi previsti dall'art. 5 del Regolamento UE, nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.

2. In particolare, i dati personali sono:

- **a.** Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (nel rispetto dei principi di liceità, correttezza e trasparenza);
- **b.** Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità (nel rispetto del principio di limitazione della finalità). Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
- **c.** Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (nel rispetto del principio di minimizzazione dei dati);
- **d.** Esatti e, se necessario, aggiornati. A tal fine sono adottate le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati (nel rispetto del

principio di esattezza);

e. Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, a condizione dell'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE (nel rispetto del principio di limitazione della conservazione);

f. Trattati in maniera da garantire un'adeguata sicurezza dei dati personali da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale, compresa la protezione, mediante misure tecniche e organizzative adeguate (nel rispetto dei principi di integrità e riservatezza).

3. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Comune adotta misure tecniche e organizzative adeguate in grado di comprovare il rispetto dei principi di cui al precedente comma (nel rispetto del principio di responsabilizzazione).

ARTICOLO 4
BASE GIURIDICA DEL TRATTAMENTO

1. Il Comune è una pubblica amministrazione ai sensi dell'art. 1, c. 2 del D. Lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. Pertanto, il trattamento di dati personali nell'esercizio dei suoi compiti istituzionali trova il fondamento di liceità nella condizione prevista dall'art. 6, par. 1, lett. b), e), f) del Regolamento UE e di regola non necessita del consenso dell'interessato.

2. Il trattamento deve sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato (principio di necessità).

ARTICOLO 5
CIRCOLAZIONE DEI DATI ALL'INTERNO DEL COMUNE

1. L'accesso ai dati conservati negli archivi del Comune da parte delle strutture e dei dipendenti del Comune è ispirato al principio della libera circolazione delle informazioni all'interno delle Direzioni in cui il Comune è organizzato e, nei casi di interesse comune, all'interno di tutto il Comune, ed è finalizzato al raggiungimento dei fini istituzionali.

2. Il Comune provvede all'organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, prevalentemente di carattere informatico, atti a facilitarne l'accesso e la fruizione.

3. L'accesso ai dati personali da parte delle strutture o dei dipendenti del Comune, connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, è soddisfatto in via diretta e senza ulteriori formalità nella misura necessaria al perseguimento dell'interesse istituzionale, ferma restando la responsabilità del richiedente derivante dall'utilizzo improprio dei dati.

ARTICOLO 6
TIPOLOGIE DI DATI TRATTATI DAL COMUNE

1. Il Comune effettua, con misure adeguate e tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto, delle finalità del trattamento, trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali, come individuate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Codice in materia di protezione dei dati personali, dal Regolamento UE, e dalle Linee guida e dai provvedimenti del Garante per la protezione dei dati personali.

2. Il Comune effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

a) Dati, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, ivi compresi i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nel Comune e relativi a:

- prove concorsuali/selezioni;
- gestione del rapporto di lavoro;
- formazione e aggiornamento professionale;
- salute e sicurezza delle persone nei luoghi di lavoro;
- strumenti di lavoro.

b) Dati relativi alle attività istituzionali, ai servizi ai cittadini, conto terzi e/o connessi ad attività trasversali:

- gestione degli spazi;
- gestione delle postazioni;
- gestione degli organi e delle cariche istituzionali;
- gestione degli infortuni;
- servizi bibliotecari;
- servizi di protocollo e conservazione documentale;
- acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso;
- servizi di posta elettronica e strumenti di comunicazione.

3. È compito dei Delegati interni o loro Referenti effettuare e documentare la ricognizione periodica dei trattamenti.

ARTICOLO 7
TITOLARE DEL TRATTAMENTO DEI DATI

1. Il Titolare del trattamento dei dati è il Comune, il cui rappresentante legale è il Sindaco pro tempore.

2. Il Comune adotta misure tecniche e organizzative adeguate al fine di garantire ed essere in grado di dimostrare la conformità del trattamento al Regolamento (UE) e al Codice in materia di protezione dei dati personali, tenendo conto della natura, dell'ambito di applicazione, del contesto, della base giuridica e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure sono periodicamente riesaminate e aggiornate.

3. Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale il Comune è responsabile del rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento (UE).

4. Il Comune coopera con il Garante per la protezione dei dati personali.

ARTICOLO 8
CONTITOLARE

1. Quando uno o più titolari del trattamento determinano congiuntamente con il Comune le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.

2. Il Comune e il Contitolare del trattamento determinano in modo trasparente, mediante un accordo interno, i rispettivi obblighi in merito all'osservanza del Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni richieste dall'Informativa privacy, salvo quanto previsto dall'art. 26 del Regolamento (UE).

3. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

4. L'interessato può esercitare i propri diritti nei confronti di ciascun contitolare del trattamento.

ARTICOLO 9

IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD) O DATA PROTECTION OFFICER (DPO)

1. Il Comune nomina un Responsabile della protezione dei dati (di seguito RPD).
2. Il RPD è figura specializzata nel supporto al Titolare e svolge la funzione di raccordo con il Garante per la protezione dei dati personali e di garante per i soggetti interessati.
3. Il RPD è individuato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti.
4. Il RPD può essere un soggetto interno (dipendente del Comune) o esterno, assolvendo in tal caso i suoi compiti in base a un contratto di servizi.
5. Il RPD è nominato, nel caso di soggetti interni, con provvedimento del Sindaco.
6. Il RPD è tenuto a svolgere i seguenti compiti:
   a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa comunitaria e nazionale relativa alla protezione dei dati;
   b) sorvegliare l'osservanza del presente Regolamento e di altre disposizioni derivanti dalla normativa comunitaria e nazionale, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
   d) cooperare con il Garante per la protezione dei dati personali;
   e) fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
   f) collaborare nella redazione e aggiornamento dei Registri di trattamento;
   g) svolgere ogni ulteriore compito attribuito dal Titolare.
7. Nell'eseguire i propri compiti il RPD considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
8. Al RPD sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione. È garantita, inoltre, una formazione permanente per permettergli l'aggiornamento costante sugli sviluppi nel settore della protezione dei dati.
9. Il RPD ha ampio accesso alle informazioni ed è interpellato per ogni problematica inerente la protezione dei dati e per ogni attività che implica un trattamento dati, fin dalla sua progettazione.
10. Il Comune garantisce che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o conflitto di interessi.
11. Il RPD non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del Regolamento UE.
12. Il Comune non rimuove o penalizza il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.
13. Il nominativo e i dati di contatto del RPD sono comunicati al Garante per la protezione dei dati personali. I dati di contatto del RPD sono inseriti nelle informative privacy e pubblicati sul sito internet istituzionale.
14. L'amministrazione costituisce a supporto del RPD una rete di Referenti che dovranno collaborare funzionalmente con il RPD, nell'ambito delle strutture nelle quali i dati personali sono gestiti per le finalità istituzionali e sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.
15. Su indicazione del RPD possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali.
16. Il RPD redige una relazione annuale dell'attività svolta.

ARTICOLO 10
RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI

1. É Responsabile esterno del trattamento qualunque soggetto esterno che esegue, in base a un contratto/convenzione o altro atto giuridico, trattamenti di dati personali per conto del Comune.
2. I Responsabili esterni del trattamento sono nominati con atto giuridico conforme al diritto nazionale e forniscono garanzie ai sensi del paragrafo 3 dell'art. 28 del Regolamento UE, in particolare per quel che riguarda le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste dallo stesso Regolamento.
3. Il Responsabile del trattamento risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
4. Negli atti di nomina i Responsabili esterno saranno autorizzati a nominare sub-responsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che lo legano al Comune e previa trasmissione dei contenuti essenziali della nomina al Comune, che potrà opporsi per motivi legittimi.
5. Qualora un sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile esterno conserva nei confronti del Comune l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.
6. Il Responsabile esterno risponde dinanzi al Comune dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

ARTICOLO 11
DELEGATI INTERNI DEL TRATTAMENTO DEI DATI PERSONALI

1. Possono essere individuati quali Delegati interni del trattamento dei dati personali, sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono, i responsabili delle strutture nell'ambito della quale i dati personali sono gestiti per le finalità istituzionali.
2. Il Delegato interno può delegare a un proprio referente i compiti di cui al successivo comma 3, relativamente ai diversi ambiti di competenza. La delega è formalizzata con apposito atto, contiene puntualmente i compiti delegati ed è corredato dalle relative istruzioni e dalla individuazione delle modalità di verifica e di controllo. Di tale delega è data comunicazione al Sindaco e al Responsabile della Protezione dei Dati, evidenza nel Registro dei trattamenti e ampia diffusione all'interno dell'amministrazione (rete intranet, ufficio personale ecc.).
3. Il Delegato interno o suo referente, opportunamente formato riguardo alle competenze anche decisionali in materia di protezione dei dati, opera con autonomia gestionale nell'ambito delle competenze affidategli, collabora funzionalmente con il RPD per l'espletamento dei seguenti compiti all'interno della propria struttura di afferenza e per gli ambiti espressamente definiti:
   - vigilare, monitorare e garantire il rispetto di quanto previsto dalle norme vigenti in materia di protezione dei dati personali;
   - rispettare ed applicare le disposizioni previste dal presente Regolamento;
   - aggiornare l'informativa privacy e la relativa modulistica;
   - collaborare, per la parte di propria competenza, nella mappatura dei trattamenti, nel censimento delle banche dati e dei trattamenti di dati esternalizzati e nella implementazione e aggiornamento del registro dei trattamenti;
   - impartire idonee istruzioni in materia di informativa privacy e di misure di sicurezza al personale incaricato del trattamento;
   - vigilare sul rispetto delle misure di sicurezza finalizzate ad evitare i rischi, anche accidentali, di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - assicurare il costante monitoraggio degli adempimenti e delle attività effettuati dai soggetti incaricati, con

particolare riferimento alla gestione della comunicazione delle violazioni di dati "data breach" e alla valutazione d'impatto privacy;

- designare per la propria struttura i soggetti incaricati, come definiti dall'art. 12 e verificare periodicamente i relativi livelli di autorizzazione;
- conservare e aggiornare l'elenco dei soggetti incaricati;
- fornire un riscontro tempestivo, per i trattamenti di competenza, nel caso di richieste di esercizio dei diritti sui dati, così come previsto dagli artt.15-22 del Regolamento UE;
- garantire l'esecuzione di ogni altra operazione richiesta o necessaria per ottemperare agli obblighi derivanti dalle disposizioni di legge e/o da regolamenti vigenti in materia di protezione dei dati personali e collaborare con l'ufficio preposto per individuare i bisogni formativi delle risorse della propria struttura;
- partecipare obbligatoriamente alle sessioni informative/formative e di sensibilizzazione in materia di protezione dei dati personali;
- segnalare al Titolare del trattamento e al RPD ogni variazione organizzativa che può avere un impatto sulle modalità di trattamento dei dati;
- per i trattamenti che hanno come base giuridica il consenso, predisporre le misure organizzative atte a garantire la conservazione della copia del consenso acquisito, sia esso cartaceo o elettronico, da parte della struttura autorizzata al trattamento;
- conservare, per quanto di propria competenza, e rendere disponibile su richiesta del Titolare o del RPD copia della seguente documentazione:
    - Accordi stipulati con i Responsabili esterni.
    - Report delle Valutazioni di impatto Privacy (DPIA).
    - Comunicazioni delle violazioni di dati personali (data breach).
    - Informative agli interessati relative ai trattamenti effettuati.

ARTICOLO 12
INCARICATI AL TRATTAMENTO

1. Gli incaricati al trattamento sono formalmente designati dal Titolare, dal Delegato interno, o dal suo referente.
2. Gli incaricati al trattamento ricevono opportuna formazione/informazione specifica in materia di trattamento dati.
3. In assenza di formale designazione con nomina individuale ad incaricati al trattamento, coloro che trattano dati che competono alla unità organizzativa cui afferiscono sono ritenuti incaricati al trattamento dei dati per documentata preposizione ad unità organizzativa e pertanto sono obbligati ad osservare quanto previsto dal presente articolo.
4. L'incaricato effettua i trattamenti dei dati personali in osservanza delle misure di sicurezza previste dal Comune, finalizzate ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati personali.
5. L'incaricato è tenuto:
    - a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante l'attività prestata;
    - a non comunicare a terzi o diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di incaricato;
    - a seguire i seminari d'informazione e formazione in materia di protezione dei dati personali e a sostenere i test finali, ove previsti per la verifica dell'apprendimento;
    - a segnalare con tempestività al responsabile del proprio ufficio e al referente eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante privacy e ai soggetti interessati.

6. L’incaricato è informato e consapevole che l’accesso e la permanenza nei sistemi informatici comunali per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari, oltre che esporre l’amministrazione a danni reputazionali.
7. L’incaricato si impegna a osservare le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica e logica adottate dal Comune.
8. Nel caso in cui non ricorrano le condizioni di cui al presente articolo, coloro che, nello svolgimento dei propri compiti, vengano a conoscenza di dati personali per i quali non possiedono esplicita autorizzazione al trattamento o che non competono alla unità organizzativa cui afferiscono, sono considerati come terzi rispetto all’amministrazione stessa, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.

ARTICOLO 13
SENSIBILIZZAZIONE E FORMAZIONE

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Comune sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo il Comune promuove l'attività formativa del personale comunale e l'attività informativa diretta a tutti coloro che hanno rapporti con il Comune.
2. Il Comune predispone ogni anno, sentito il RPD, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata.
3. La frequenza delle attività di formazione è obbligatoria.

ARTICOLO 14
INFORMATIVA

1. Per ogni tipologia di trattamento dei dati il Comune fornisce l’informativa all’interessato, anche mediante rinvio all’informativa presente sul sito del comune o altro strumento facilmente accessibile, salvo il caso in cui l’interessato sia già in possesso delle informazioni (art. 13, par. 4 del Regolamento UE) o in altri casi particolari previsti dall’art. 14, par. 5 del Regolamento UE. L’informativa fornita all’interessato deve essere concisa, trasparente, intellegibile, facilmente accessibile e usare un linguaggio chiaro e semplice.
2. L’informativa deve contenere:
   - i dati di contatto del Comune;
   - i dati di contatto del Responsabile della Protezione dei Dati personali;
   - le finalità del trattamento;
   - la base giuridica del trattamento ai sensi dell’art. 4;
   - gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l’interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
   - l’eventuale volontà del Comune di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di un fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai resi disponibili;
   - il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;
   - i diritti che l’interessato può esercitare, quali: l’accesso ai dati personali, la rettifica o la cancellazione degli

stessi, la limitazione del trattamento o l'opposizione, il diritto alla portabilità dei dati, la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, il diritto di proporre reclamo al Garante per la protezione dei dati personali;

- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.

3. Nel caso in cui i dati non siano raccolti presso l'interessato, il Comune si riserva la possibilità di non fornire l'informativa nel caso in cui l'interessato già disponga delle informazioni oppure comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.

4. L'informativa può essere fornita in forma semplificata nei casi consentiti dalla normativa vigente.

5. L'informativa può non essere fornita nel caso in cui si prefiguri il rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.

6. Le informative di competenza delle strutture sono aggiornate dai Delegati interni o loro Referenti.

7. Il personale e chiunque operi sotto l'autorità del Comune può trattare i dati personali solo per le specifiche finalità indicate nell'informativa fornita all'interessato al momento del conferimento dei dati o per ogni altra finalità prevista dalla legge. I dati personali non possono essere usati per finalità diverse da quelle per le quali sono stati raccolti. Se si rendesse necessario modificare le finalità del trattamento, l'interessato dovrà essere informato della nuova finalità prima dell'inizio di qualunque trattamento. Fanno eccezione a questa disposizione i trattamenti effettuati per finalità di ricerca.

ARTICOLO 15
DIRITTI DELL'INTERESSATO

1. Il Comune garantisce il rispetto dei diritti degli interessati di cui agli artt. da 12 a 22 del Regolamento UE. In particolare, l'interessato può:

a) ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;

b) ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento;

c) esercitare il diritto alla limitazione del trattamento in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, nonché nel periodo necessario al titolare per riscontrare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione è consentita la conservazione dei dati ed i trattamenti legittimati dal consenso dell'interessato, dalla necessità di accertamento dei diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante;

d) esercitare il diritto di opposizione alla profilazione;

e) esercitare il diritto alla portabilità dei dati qualora il trattamento si basi sul consenso ai sensi dell'art. 6. par. 1, lettera a), o dell'art. 9, par. 2, lettera a) del Regolamento UE o su un contratto ai sensi dell'art. 6, par. 1, lettera b) del Regolamento UE e sia effettuato con mezzi automatizzati. Tale diritto non si applica al trattamento necessario per l'esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune;

f) esercitare il diritto all'oblio chiedendo la cancellazione dei propri dati personali. Tale diritto può essere esercitato ove ricorra una delle seguenti fattispecie:

- **I.** i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
- **II.** l'interessato revoca il consenso su cui si basa il trattamento;
- **III.** l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

IV. i dati personali sono trattati illecitamente;

V. adempimento di un obbligo legale;

VI. i dati riguardino minori.

Il Comune informa della richiesta di cancellazione ogni altro titolare e responsabile che tratta i dati personali di cui è chiesta la cancellazione.

2. L'interessato può esercitare i suoi diritti con richiesta scritta indirizzata all'Ufficio Relazioni con il Pubblico, al responsabile della struttura competente per la gestione dei dati personali oggetto della richiesta o, in alternativa, al Delegato interno o suo referente.
3. Il riscontro alla richiesta presentata dall'interessato viene fornito dal Delegato interno entro 30 giorni dalla data di acquisizione della richiesta al Protocollo, anche nei casi di diniego. Per i casi di particolare e comprovata difficoltà il termine dei 30 giorni può essere esteso fino a 3 mesi, non ulteriormente prorogabili. Di tale proroga viene data informazione all'interessato entro 30 giorni dalla acquisizione della richiesta al Protocollo.
4. Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.
5. Il Comune agevola, per il tramite dei Delegati interni o loro referenti, l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa.
6. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.
7. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, il Comune può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi sostenuti oppure può rifiutare di soddisfare la richiesta.
8. La modulistica per l'esercizio dei sopra citati diritti è redatta e aggiornata a cura dei Delegati interni o loro referenti che devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi, nei casi più complessi, del supporto del RPD.
9. Le richieste di esercizio di diritti da parte degli interessati sono inserite all'interno di un Registro entro e non oltre 30 giorni dalla data di conclusione del procedimento.
10. Nei casi di trattamenti di dati esternalizzati, all'atto della nomina il Responsabile esterno è vincolato a collaborare con il Comune.

ARTICOLO 16
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

1. È vietato trattare dati personali atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di 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, fatti salvi i seguenti casi:
   a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
   b. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, ai sensi dell'art. 20;
   c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   e. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
   f. il trattamento è necessario per motivi di interesse pubblico rilevante ai sensi dell'art. 2-sexies del Codice in materia di protezione dei dati personali.
2. I dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento solo in conformità alle misure di garanzia disposte e adottate con apposito provvedimento dal Garante per la protezione dei dati

personali.

ARTICOLO 17
TRATTAMENTO DI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

1. Il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, ai sensi dell'art. 2-octies del Codice in materia di protezione dei dati personali.

ARTICOLO 18
ACCESSO AI DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO

1. I limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e per l'esercizio dell'accesso civico restano disciplinati rispettivamente dalla legge 7 agosto 1990, n. 241 e successive modificazioni e dal decreto legislativo 14 marzo 2013, n. 33 e successive modificazioni e dai Regolamenti comunali in materia.

2. Quando il trattamento riguarda categorie particolari di dati personali come elencate all'art. 16, l'accesso è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

ARTICOLO 19
COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI

1. La comunicazione e la diffusione dei dati personali sono permesse quando:
- **a.** siano previste da norme di legge, di regolamento o dal diritto dell'Unione europea;
- **b.** siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o aggregati;
- **c.** siano richieste per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia;
- **d.** siano necessarie per il soddisfacimento di richieste di accesso ai sensi dell'art. 18.

2. È esclusa la comunicazione a terzi di dati relativi a origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, 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, dati relativi a condanne penali e a reati.

3. La comunicazione di dati a soggetti pubblici è sempre ammessa per i fini istituzionali e ove prevista da norma di legge o regolamento.

4. Le richieste da parte di soggetti privati ed enti pubblici economici volte ad ottenere la comunicazione di dati, devono essere formulate per iscritto e motivate e devono contenere:
- il nome, la denominazione o la ragione sociale del richiedente;
- l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate.

5. Il Comune, nella figura del Delegato interno o suo referente, valuta eventuali richieste di comunicazione o diffusione di dati personali a soggetti privati e decide in ordine all'opportunità di effettuare la comunicazione sulla base di quanto disposto dalle norme vigenti in materia di protezione dei dati personali e di quanto previsto dal presente Regolamento.

6. Le modalità di comunicazione dei predetti dati, per la quale può essere richiesto un contributo a copertura dei costi sostenuti, sono decise dal Comune.

7. Il Comune può comunicare a enti pubblici e privati i dati necessari alla gestione del rapporto di lavoro, relativi al personale trasferito, comandato, distaccato o comunque assegnato in servizio a un ente diverso da quello di

appartenenza.

ARTICOLO 20
TRATTAMENTI NELL'AMBITO DEL RAPPORTO DI LAVORO

1. Il Comune effettua il trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi.
2. Il trattamento dei dati relativi ai dipendenti da parte del Comune non richiede il consenso esplicito in quanto il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
3. Il Comune garantisce ai dipendenti l'esercizio dei diritti previsti dagli articoli da 12 a 22 del Regolamento UE, compreso il diritto di accesso ai dati valutativi di natura soggettiva, nonché il diritto all'informativa.
4. Il Comune adotta misure tecniche e organizzative atte a garantire la tutela delle prerogative individuali e sindacali come disposte dalla normativa, in particolare dallo Statuto dei lavoratori e dalle norme che lo richiamano, oltre che dalle regole deontologiche promosse dal Garante per la protezione dei dati personali.
5. Il Comune può comunicare a soggetti pubblici e privati dati comuni del personale che, in ragione di una qualità professionale specifica, usufruisce di corsi di formazione forniti in accordo con altri Enti pubblici, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.
6. Il Comune comunica i dati del personale addetto alla sicurezza sui luoghi di lavoro a soggetti pubblici e privati che contribuiscono alla formazione su tali tematiche.
7. Nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile, successivo all'invio del curriculum stesso.
8. Non è dovuto il consenso al trattamento dei dati personali presenti nei curricula quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

ARTICOLO 21
DIFFUSIONE DEI RISULTATI DI CONCORSI E SELEZIONI

1. In ottemperanza ai principi di trasparenza cui il Comune si ispira, è consentita la pubblicazione di esiti di prove concorsuali e selettive, anche sui siti web del Comune, nei limiti previsti dalla normativa vigente.
2. La pubblicazione dei dati sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati e per un periodo di tempo non superiore a sei mesi.

ARTICOLO 22
TRATTAMENTO AI FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE O DI RICERCA STORICA

1. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.
2. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto del principio della minimizzazione dei dati.
3. Ove possibile e senza pregiudicare il raggiungimento delle finalità del trattamento, i dati dovranno essere trattati con misure tecniche che non consentano più di identificare l'interessato.
4. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati

anche per altre finalità secondo i principi stabiliti dall'articolo 5 del Regolamento UE.

5. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto delle regole deontologiche in materia approvate dal Garante per la protezione dei dati personali.

ARTICOLO 23
TRATTAMENTO AI FINI STATISTICI O DI RICERCA SCIENTIFICA

1. Il trattamento di dati personali ai fini statistici o di ricerca scientifica da parte di chiunque operi all'interno di uffici e strutture del Comune o per conto del Comune stesso, deve avvenire nel rispetto dei seguenti principi:

a) i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né trattati per altri scopi;

b) all'interessato deve essere fornita puntuale informazione relativamente alle finalità statistiche o di ricerca scientifica del trattamento ai sensi dell'art. 14, a meno che questo non richieda uno sforzo sproporzionato rispetto al diritto tutelato e sempre che siano adottate le idonee forme di pubblicità individuate dalle regole deontologiche in materia, promosse dal Garante.

2. Fuori dei casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di categorie particolari di dati personali, quando richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-septies del Codice in materia di protezione dei dati personali.

ARTICOLO 24
SICUREZZA

1. Il Comune mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al probabile rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati personali.

2. Nel valutare l'adeguato livello di sicurezza, il Comune tiene conto dei rischi 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.

3. Il Comune effettua la valutazione dei rischi connessi al trattamento e adotta idonee misure di sicurezza comprendenti, ove opportuno:

- la pseudonimizzazione e la cifratura dei dati:
- le misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni;
- la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4. Le misure tecniche sono riesaminate in modo periodico e sono illustrate nelle sessioni formative.

5. Il Comune considera rischioso il trasporto di dati personali su ogni supporto (computer portatili, copie cartacee, pendrive ecc.). Ciò vale prioritariamente per le categorie particolari di dati, i grandi volumi di dati personali e le informazioni che comportano particolari rischi per l'interessato nel caso di perdita o distruzione. Solo in circostanze eccezionali tali dati possono essere trasportati fuori dagli ambienti del Comune e sotto la diretta responsabilità di personale autorizzato. In particolare, il personale autorizzato è tenuto a:

- ove possibile fare uso di accesso remoto tramite login e password alle informazioni;
- trasportare solo la quantità minima di dati personali;
- assicurarsi che i dispositivi mobili e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali fuori dagli ambienti comunali siano dotati di sistemi di crittografia.

6. Qualunque perdita e/o furto di dati deve essere tempestivamente segnalato e trattato secondo la procedura di gestione delle violazioni di dati personali di cui all'art. 27.

7. Per quanto non espressamente disciplinato dal presente articolo sulla sicurezza, si fa rinvio a quanto disposto dai regolamenti del Comune e dalle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte da AgID, Agenzia per l'Italia Digitale.

ARTICOLO 25
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

1. Il Comune istituisce e aggiorna un Registro delle attività di trattamento svolte sotto la propria responsabilità.

2. Il Registro censisce le attività di trattamento svolte dagli uffici e dalle strutture del Comune e le principali caratteristiche dei trattamenti. Il registro è costantemente aggiornato, pubblicato nella rete intranet del Comune e, su richiesta, messo a disposizione del Garante per la protezione dei dati personali.

3. Nel Registro sono elencati e descritti sia i trattamenti dei quali il Comune è Titolare sia i trattamenti che il Comune effettua in qualità di Responsabile esterno di altri titolari.

a) Il Registro dei trattamenti dei quali il Comune è Titolare contiene le seguenti informazioni:

- il nome ed i dati di contatto del Comune e del RPD;
- le finalità del trattamento;
- la 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;
- ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

b) Il Registro dei trattamenti svolti dal Comune per conto di altri Titolari e per i quali il Comune si configura come Responsabile contiene le seguenti informazioni:

- il nome ed i dati di contatto del Comune e del RPD;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- 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'art. 49 del Regolamento UE, la documentazione delle garanzie adeguate;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

ARTICOLO 26
LA VALUTAZIONE DI IMPATTO

1. Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, il Delegato interno o suo referente, previa consultazione con il RPD, effettua una valutazione dell'impatto sulla protezione dei dati personali.

2. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.

3. La valutazione d'impatto sulla protezione dei dati è obbligatoria nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali quali: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di 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, dati relativi a condanne penali e a reati;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza);

d) il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

4. Il Delegato interno o suo referente si consulta con il RPD anche per assumere la decisione di effettuare o meno la valutazione di impatto. Tale consultazione e le conseguenti decisioni assunte dal Delegato interno o suo referente devono essere documentate nell'ambito della valutazione di impatto. Il Delegato interno o suo referente è tenuto a documentare le motivazioni nel caso adotti condotte difformi da quelle raccomandate dal RPD.

5. Il Comune, per il tramite del RPD, consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della valutazione di impatto (DPIA) condotta indicano l'esistenza di un rischio residuale elevato.

6. Il Comune, per il tramite del RPD, consulta il Garante per la Protezione dei dati personali 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.

ARTICOLO 27
VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

1. Si intende per violazione dei dati personali una violazione di sicurezza 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.

2. Al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati, il Comune in qualità di Titolare del trattamento definisce una procedura di gestione delle violazioni di dati personali, contenuta in apposito "Manuale per la gestione degli incidenti di sicurezza in ordine ai dati personali trattati dal Comune di Jesolo", allegato A) al presente regolamento.

3. Tale procedura si applica a qualunque attività svolta dal Comune con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.

4. La procedura definisce le modalità per identificare la violazione, analizzare le cause della violazione, definire le misure da adottare per rimediare alla violazione dei dati personali, attenuarne i possibili effetti negativi, registrare le informazioni relative alla violazione, identificare le azioni correttive e valutarne l'efficacia, notificare la violazione di dati personali al Garante nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche, comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio sia elevato.

5. La procedura costituisce una delle materie oggetto della formazione del personale di cui all'art 13.

6. Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa può 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.

ARTICOLO 28
VIDEOSORVEGLIANZA

1. Il trattamento dei dati personali effettuato mediante l'attivazione di impianti di videosorveglianza negli ambienti del Comune si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.

2. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nella regolamentazione del Comune in materia di videosorveglianza e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria.

3. Il Comune garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza attraverso l'adozione di apposito "Regolamento per l'esercizio dei sistemi di videosorveglianza".
4. Resta ferma la necessità di effettuare una valutazione di impatto (DPIA), ai sensi dell'art. 27, comma 3, lettera c), ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.
5. Non è consentito, nel pieno rispetto dello Statuto dei lavoratori, l'uso di impianti e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

ARTICOLO 29
SANZIONI AMMINISTRATIVE

1. Fermo restando quanto previsto dagli articoli 58, 82, 83 e 84 del Regolamento UE e dal Codice in materia di protezione dei dati personali, le sanzioni disciplinari e amministrative a carico del personale in caso di violazione delle leggi e delle procedure in tema di protezione dei dati personali saranno definite dal Comune anche sulla base di quanto disposto dai CCNNLL, dal Codice etico e dai Codici di comportamento.

ARTICOLO 30
TRATTAMENTO DEI DATI NELLE SEDUTE DEGLI ORGANI COLLEGIALI DEL COMUNE

1. Nelle sedute degli Organi Collegiali del Comune il trattamento dei dati avviene in conformità al presente Regolamento e al regolamento disciplinante le attività degli organi collegiali.

ARTICOLO 31
DISPOSIZIONI FINALI

1. Dalla data di entrata in vigore del presente Regolamento, devono intendersi abrogate tutte le norme regolamentari e statutarie incompatibili in relazione a soggetti e materie interessate al trattamento.
2. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento (UE) 2016/679 e del D. Lgs. 196/2003 Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dal Garante.
3. Costituiscono parte integrante e sostanziale del presente Regolamento tutti gli allegati che ad esso si riferiscono in quanto connessi ad ambiti specifici in esso contenuti, anche redatti successivamente alla sua emanazione, nonché gli altri atti espressamente richiamati.

ARTICOLO 32
CONTROLLI PERIODICI

1. La sicurezza può essere compromessa da una serie di eventi, che devono essere tracciati ed essere oggetto di analisi periodica.
2. La tracciatura degli eventi verrà effettuata compilando il Modello MMS – Modello per il Monitoraggio della Sicurezza, generalmente con frequenza trimestrale e con frequenza quindicinale per i servizi che il Comune ritiene più esposti ai rischi; il modello compilato deve essere inviato al Dirigente del Settore all'interno del quale è incardinato il Servizio Sistemi Informativi e al Responsabile della protezione dei dati.

ARTICOLO 33
DOCUMENTO SUL MONITORAGGIO DELLA SICUREZZA

1. Gli eventi di cui all'articolo precedente verranno analizzati all'interno di un documento denominato DMS – Documento per il Monitoraggio della Sicurezza, predisposto dal Responsabile della protezione dei dati e posto

all'attenzione del Titolare del Trattamento. All'interno del DMS devono inoltre trovare trattazione esaustiva ed organica tutte le problematiche relative alla sicurezza e alla protezione dei dati personali che si sono verificate nel trimestre di riferimento, come ad esempio:

a. l'esternalizzazione di un nuovo trattamento di dati
b. la predisposizione di una procedura operativa o di un regolamento ad-hoc
c. la predisposizione di una lettera di nomina
d. la predisposizione di una nuova informativa
e. la predisposizione di comunicazioni ai dipendenti o agli interessati
f. il recepimento di norme o linee guida emesse a livello nazionale od europeo, concernenti la sicurezza o la protezione dei dati
g. l'analisi di una richiesta di accesso ai dati
h. la revisione del Registro del trattamenti dei dati
i. lo svolgimento di un DPIA – Data Protection Impact Assessment
j. la verifica del soddisfacimento dei principi di Privacy by Design e Privacy by default all'interno di un sistema o di un processo.

2. Ove necessario, il Responsabile per la protezione dei dati segnala al Titolare eventuali criticità e fatti rilevanti ai fini dell'adeguamento delle policy del Comune, a maggior tutela dei dati personali.

ARTICOLO 34
EFFICACIA TEMPORALE E PUBBLICITA'

1. Il Comune provvede a dare pubblicità al presente Regolamento ed alle successive modifiche ed integrazioni mediante pubblicazione sul sito Web del Comune.

Allegato A)

MANUALE PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA IN ORDINE AI DATI PERSONALI TRATTATI DAL COMUNE DI JESOLO

Scopo/Premessa

Il Comune di Jesolo (d'ora in avanti anche solo Comune) protegge la sicurezza e la riservatezza delle Informazioni Personali di qualsiasi Interessato e fornisce immediata risposta agli Incidenti di Sicurezza, da intendersi come qualsiasi incidente di sicurezza che coinvolge Dati Personali, come di seguito meglio definiti.

Qualsiasi Incidente di sicurezza, da chiunque rilevato presso il Comune, deve essere gestito secondo le modalità definite nelle pagine seguenti.

L'obiettivo del presente documento è:

- sensibilizzare il personale sulle responsabilità in materia di protezione dei dati personali e sull'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli Incidenti di sicurezza;
- definire processi per identificare, tracciare e reagire ad un Incidente di sicurezza, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se si renda necessario procedere alla notifica al Garante e alla comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli Incidenti di sicurezza;
- assicurare un adeguato flusso comunicativo all'interno del Comune tra le parti interessate.

A. Definizioni

Dati personali	Qualunque informazione relativa ad una persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (per es. n. di matricola), i dati relativi all'ubicazione, un identificativo on line. Si considera identificabile la persona fisica che può essere identificata anche tramite uno o più elementi della sua identità fisica, psichica, economica, culturale, sociale.
Dati biometrici	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.
Dati comuni	Categoria non definita nella normativa. Fanno parte dei dati comuni il codice fiscale, il numero di partita IVA, la residenza, il numero di telefono, l'indirizzo e-mail.
Dati giudiziari	Dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u) del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli art. 60 e 61 del codice di procedura penale.
Dati particolari	Dati personali idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti politici, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati genetici, biometrici e i dati idonei a rivelare lo stato di salute e la vita sessuale.

Dati relativi alla salute	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.
Comunicazione	Rivelazione di dati personali a uno o più enti identificati e diversi dal Soggetto Interessato, rappresentante del titolare del trattamento nel territorio statale, responsabile del trattamento e soggetti responsabili dell'elaborazione sotto qualsiasi forma, incluso il rendere disponibili o accessibili tali dati.
Garante	L'Autorità Garante per la protezione dei dati personali.
Incidente di sicurezza	Violazione della sicurezza che può anche non riguardare le Informazioni Personali.
Interessato	Qualsiasi persona fisica a cui si riferiscono i dati personali.
Responsabile della protezione dei Dati o DPO	Soggetto individuato dal Titolare in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati che deve essere necessariamente coinvolta in tutte le questioni che riguardano la protezione dei dati personali.
Titolare del trattamento	Persona fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza.
Trattamento	Qualsiasi operazione o serie di operazioni eseguite con o senza l'ausilio di mezzi elettronici o automatici che riguarda la raccolta, registrazione, organizzazione, mantenimento, interrogazione, elaborazione, modifica, selezione, recupero, confronto, utilizzo, interconnessione, blocco, comunicazione, divulgazione, cancellazione e distruzione di dati, che questi siano o meno contenuti in una banca dati.
Violazione di dati	Violazione della sicurezza che comporta, in modo accidentale o illecito, la distruzione, perdita, alterazione, comunicazione non autorizzata di, o accesso a, dati personali trasmessi, conservati o altrimenti trattati. La violazione dei dati è quindi un incidente di sicurezza che riguarda le Informazioni Personali.

B. Ambito di applicazione

La presente procedura si applica a tutte le Informazioni Personali e alle altre informazioni che, pur non costituendo Informazioni Personali, sono raccolte o gestite o comunque trattate da Comune, siano esse dati contenuti su dispositivi elettronici, accessibili via rete o web, contenuti su dispositivi mobili o portatili ovvero su supporti cartacei.

C. Ruoli e tipologie di *Personal Data Breach*

La tempestività è un fattore determinante nella risposta agli Incidenti di sicurezza e ai *Personal Data Breach* ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

Coerentemente con il concetto di sicurezza (Riservatezza, Disponibilità e Integrità), gli incidenti possono avere per oggetto uno o più di questi attributi. Laddove interessino uno solo dei sotto indicati attributi, questi vengono classificati in:

1. *Personal Data Breach* sulla Riservatezza: violazione della riservatezza delle Informazioni Personali (a titolo esemplificativo: quando si verifica una comunicazione non dovuta o un accesso non autorizzato o accidentale ai dati personali);
2. *Personal Data Breach* sulla Disponibilità: quando i dati personali non sono disponibili perché si verifica una loro perdita accidentale o una distruzione (a titolo esemplificativo viene smarrita la chiave di

decriptazione dell'unica copia di dati criptati e non è disponibile una copia di *backup*). La perdita di disponibilità può anche essere temporanea (e configurare, comunque, un *Personal Data Breach*), vista l'importanza di avere informazioni disponibili in un dato momento;

3. *Personal Data Breach* sull'Integrità: quando si verifica una alterazione non autorizzata o accidentale dei dati personali.

D. Procedure a tutela della sicurezza dei dati

1) Preparazione

Presso il Comune sono state attivate procedure a tutela della sicurezza dei dati, tra cui:

- l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di Incidente di sicurezza;
- l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, di sicurezza dei Dati Personali e dei Sistemi;
- la predisposizione di un sistema di protezione, mediante apposite misure tecniche (*firewall*, *antivirus*…) dell'accesso a Internet e ai dispositivi elettronici.

Il personale e i collaboratori che prestano attività in Comune, ove dovessero venire a conoscenza di un Incidente di sicurezza o di elementi che fanno sospettare (anche a seguito di segnalazione di terzi) che si sia verificato o possa verificarsi un tale incidente, sono tenuti a comunicare immediatamente tale circostanza all'Ufficio Sistemi Informativi.

Il pubblico, per segnalare eventuali anomalie o disservizi, potrà contattare l'Ufficio Relazioni con il Pubblico (URP) che, a sua volta, dovrà informare immediatamente l'Ufficio Sistemi Informativi.

2) Risposta: norme generali

La risposta a un Incidente di sicurezza o a un *Personal Data Breach* deve avvenire secondo le fasi descritte di seguito. Considerando, tuttavia, che gli Incidenti possono avere molteplici cause o coinvolgere diversi soggetti ed avere conseguenze caratterizzate da vari livelli di gravità, tali fasi potrebbero sovrapporsi o richiedere tempistiche differenti o aggiornamenti.

Considerati i rischi e, in caso di *Personal Data Breach*, le ridotte tempistiche per effettuare la Notifica e per la comunicazione agli interessati, **occuparsi degli Incidenti di sicurezza deve essere obiettivo prioritario per tutti i soggetti coinvolti nella loro gestione**.

Tutti gli Incidenti di sicurezza e i *Personal Data Breach* devono essere trattati con il massimo livello di riservatezza: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

3) Rilevazione

Nel caso in cui si sia verificato un Incidente di sicurezza o si abbia il sospetto di un incidente, le azioni da seguire sono le seguenti:

a) dovrà essere avvertito l'Ufficio Sistemi Informativi per gli approfondimenti necessari e per l'identificazione della natura dell'evento. L'amministratore di sistema dell'Ufficio Sistemi Informativi documenta l'evento in un registro, assegna un numero di riferimento e inserisce tutte le informazioni in suo possesso quali data, orario, luogo, fonte della segnalazione, sistema ed entità della violazione;

b) l'amministratore di sistema dopo aver valutato l'evento contatta via email ed anche via telefono il Dirigente dell'Ufficio Sistemi Informativi ed il Responsabile della protezione dei dati (DPO); inoltre in caso di *Data Breach* cartacei contatta il Dirigente del settore presso il quale si è verificato il *Data Breach* (d'ora in avanti anche solo Dirigente del settore competente)

c) il Responsabile della protezione dei dati è incaricato di intraprendere delle azioni tempestive per risolvere il problema. In caso di sua assenza, nel caso di *Data Breach* informatici il Responsabile della protezione dei dati potrà incaricare il Dirigente dell'Ufficio Sistemi Informativi, in caso di *Data Breach* cartacei il Sindaco potrà incaricare il Dirigente del settore competente;

d) il Responsabile della protezione dei dati, in caso di *Data Breach* informatici in collaborazione con il Dirigente dell'Ufficio Sistemi Informativi ed in caso di *Data Breach* cartaceo in collaborazione con il Dirigente del settore competente, coordina le fasi di valutazione e risoluzione, di seguito definite, compresa l'organizzazione di riunioni, comunicazioni interne, relazioni sulle informazioni raccolte e informative su ogni altra misura intrapresa per la gestione dell'Incidente di sicurezza. In particolare, il Responsabile della protezione dei dati dovrà immediatamente avviare le necessarie verifiche al fine di appurare se si sia effettivamente verificato un Incidente di sicurezza, valutandone la probabilità e gravità. Il Responsabile della protezione dei dati può incaricare un soggetto esterno qualificato per avere conferma della sussistenza di un Incidente di sicurezza.

4) Valutazione e contenimento

Valutazione Preliminare

Il Responsabile della protezione dei dati effettua immediatamente una valutazione preliminare, al fine di determinare se si sia effettivamente verificato un incidente di sicurezza e determina, inoltre, se quest'ultimo possa qualificarsi anche come *Personal Data Breach*. Al termine di tale valutazione preliminare, il Comune si considera "venuto a conoscenza" della violazione e, conseguentemente, da tale momento inizieranno a decorrere i termini per la notifica e la comunicazione.

A tal fine il Responsabile della protezione dei dati, in caso di *Data Breach* informatici in collaborazione con il Dirigente e l'amministratore di sistema dell'Ufficio Sistemi Informativi ed in caso di *Data Breach* cartacei in collaborazione con il Dirigente del settore competente, dovrà per quanto possibile:

- in caso di *Data Breach* informatici: identificare il dispositivo (computer, apparato di rete, apparato mobile, sistema di *backup*, etc...) colpito
- identificare la causa, l'entità, la tipologia di dati o di Informazioni personali coinvolte e la sensibilità delle informazioni;
- verificare la natura dei soggetti coinvolti (es: dipendenti, cittadini, imprese) e il loro numero;
- verificare se i dati e le Informazioni personali non siano più disponibili ovvero rimangano comunque accessibili e utilizzabili dal Comune;
- stabilire se l'infrazione sia stata intenzionale, colposa o accidentale;
- valutare se l'incidente possa causare danni agli Interessati e determinare la probabilità e gravità del danno;
- individuare eventuali misure che permettano di trattare il rischio.

Inoltre, il Responsabile della protezione dei dati, valuta, secondo i criteri stabiliti nelle tabelle di cui al paragrafo F, il livello di rischio per gli Interessati (basso, medio, alto o molto alto) di pregiudizio/lesione dei diritti e alle libertà fondamentali derivante dalla violazione.

Comunicazione dei risultati dell'*assessment*

Il Responsabile della protezione dei dati informa, ove possibile entro le 24 ore, il Sindaco e l'Ufficio Assicurazioni-Gestione sinistri-Contenzioso giudiziario sull'evento, sui progressi della valutazione e sul livello di

gravità della violazione. Nel caso di *Personal Data Breach* conclamato, il Sindaco, con il parere del Responsabile della protezione dei dati, stabilisce se procedere alla notificazione al Garante e alla comunicazione ai soggetti interessati entro i termini sotto indicati.

Decisioni in merito alla notifica al Garante e alla comunicazione agli Interessati

La decisione sarà basata sul livello di rischio secondo quanto segue. Se il livello di rischio è:

- **Nullo/Basso**: non verrà effettuata la notifica al Garante né la comunicazione ai soggetti interessati. L'incidente/*Personal Data Breach* dovrà essere comunque registrato dal Responsabile della protezione dei dati nell'apposito registro di cui al paragrafo E e dovranno essere avviate le necessarie contromisure per prevenire eventuali ulteriori incidenti;
- **Medio, Elevato o Molto elevato**, il Sindaco notificherà il *Personal Data Breach* al Garante;
- **Elevato o Molto elevato**, il Sindaco comunicherà il *Personal Data Breach* agli Interessati secondo quanto indicato al punto 6.

Il Responsabile della protezione dei dati, in caso di *Data Breach* informatici in collaborazione con il Dirigente e l'amministratore di sistema dell'Ufficio Sistemi Informativi ed in caso di *Data Breach* cartacei in collaborazione con il Dirigente del settore competente, intraprenderà azioni immediate per contenere o prevenire ulteriori danni, quali, ad esempio, limitare l'accesso a documenti o sistemi, mettere fuori servizio sistemi e reti, bloccare una porta o un indirizzo IP internamente o esternamente. Tali restrizioni rimarranno in essere fino alla risoluzione dell'incidente.

5) Risoluzione

Il Responsabile della protezione dei dati è responsabile della risoluzione dell'incidente e del *Personal Data Breach*, avvalendosi anche della collaborazione del Dirigente dell'Ufficio Sistemi Informativi in caso di *Data Breach* informatici e del Dirigente del settore competente in caso di *Data Breach* cartacei, e stabilisce se è necessario l'intervento di risorse esterne. Le fasi di risoluzione comprendono:

- determinazione della causa e dell'ambito;
- individuazione dei dati, sistemi e dispositivi compromessi;
- gestione o attenuazione della causa della violazione;
- in caso di *Data Breach* informatici: localizzazione, reperimento e conservazione (ove possibile) di tutti i *log* e *record* elettronici (inclusi *backup*, immagini, *hardware*, etc...) e di videosorveglianza per successive fasi legali; l'apposizione della firma digitale e la marcatura temporale di tutte le evidenze informatiche disponibili;
- nel caso di sospetta attività criminale, comunicazione all'Ufficio Assicurazioni-Gestione sinistri-Contenzioso giudiziario e segnalazione alle autorità competenti, ove previsto;
- valutazione di tutte le alternative per sostituire o ripristinare risorse e macchinari compromessi, inclusi costi di riparazione o ripristino dei beni a livelli di sicurezza accettabili.

In nessun caso l'accesso ai dati o il ripristino di un sistema compromesso tornerà a una regolare operatività senza previa approvazione del Responsabile della protezione dei dati, del Sindaco e del Dirigente dell'Ufficio Sistemi Informativi in caso di *Data Breach* informatici e del Dirigente del settore competente in caso di *Data Breach* cartacei.

Ulteriori attività di risoluzione subordinate al tipo di incidente e di dati compromessi, non descritte nel presente documento, verranno stabilite e gestite dal Responsabile della protezione dei dati.

Il Responsabile della protezione dei dati comunica l'incidente e le misure risolutive adottate al Sindaco e al Dirigente dell'Ufficio Sistemi Informativi in caso di *Data Breach* informatici e del Dirigente del settore competente in caso di *Data Breach* cartacei. Il Responsabile della protezione dei dati e i citati soggetti stabiliscono quando ritenere l'incidente risolto e, quindi, chiuso.

Il Responsabile della protezione dei dati, in collaborazione con il Dirigente dell'Ufficio Sistemi Informativi in caso di *Data Breach* informatici e del Dirigente del settore competente in caso di *Data Breach* cartacei, gestisce le azioni correttive per prevenire problemi futuri, compresi:

- revisione dei livelli di sicurezza delle informazioni e dei programmi di formazione;
- conduzione di audit di sicurezza fisica e tecnica;
- revisione delle politiche e procedure del Comune;
- revisione delle pratiche di selezioni dei dipendenti e di tirocinio;
- revisione dei fornitori di servizi.

6) Comunicazione all'esterno: notifica al Garante e comunicazione agli Interessati

Notifica al Garante

Il Sindaco, con il supporto del Responsabile della protezione dei dati, provvede alla Notifica al Garante quando non è "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche". Tale valutazione dovrà essere effettuata utilizzando le tabelle riportate al paragrafo F.

Il Sindaco, con il supporto del Responsabile della Protezione Dati, notifica il *Personal Data Breach* al Garante, **senza ingiustificato ritardo e, ove possibile, entro 72 ore** da quando si è avuto conoscenza del *Personal Data Breach*, utilizzando il modulo messo a disposizione dal Garante. Il modulo va compilato con firma digitale e inviato via email o posta elettronica certificata all'indirizzo che messo a disposizione dal Garante.

Quando, in funzione della natura del *Personal Data Breach*, a seguito dell'*assessment* preliminare di cui al precedente punto 4, pur avendo valutato la sussistenza di un *Personal Data Breach*, non è possibile fornire le informazioni di cui ai moduli sopra indicati entro i termini previsti (perché ad esempio, in caso *di cyber attack*, devono essere condotte analisi approfondite per stabilire la natura del *Personal Data Breach* e/o il numero o le categorie dei soggetti coinvolti), il Sindaco, con il supporto del Responsabile della protezione dati, sentito il Dirigente dell'Ufficio Sistemi Informativi in caso di *Data Breach* informatici e del Dirigente del settore competente in caso di *Data Breach* cartacei, procede ad una notifica parziale. Quest'ultima dovrà essere successivamente integrata senza ingiustificato ritardo (notifica per fasi). In questo caso, senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando si è avuto conoscenza del *Personal Data Breach*, dovrà essere notificato al Garante che si è verificato un possibile *Personal Data Breach*, precisando che verranno successivamente fornite maggiori informazioni. Dovranno essere anche fornite le ragioni per cui si ricorre alla Notifica per fasi.
Il Sindaco, avvalendosi del supporto del Responsabile della protezione dati, ove a seguito di una prima notifica dovesse appurare che in realtà non si è verificato alcun *Personal Data Breach* deve comunicare tale circostanza al Garante.

Comunicazione ai Soggetti Interessati

Il Sindaco, con il supporto del Responsabile della protezione dei dati, provvede alla comunicazione ai soggetti interessati dal *Personal Data Breach* quando la violazione è suscettibile di presentare un **rischio elevato** per i loro diritti e libertà fondamentali. Anche tale valutazione dovrà essere effettuata utilizzando le tabelle riportate al paragrafo F.

La comunicazione ai soggetti interessati deve avvenire nel più breve tempo possibile e senza ingiustificato ritardo, al fine di permettere a questi ultimi di adottare le necessarie contromisure per limitare i danni. In caso di urgenza, si può rendere necessario procedere alla comunicazione agli Interessati anche prima di aver effettuato la notifica al Garante.

Il Sindaco, avvalendosi del supporto del Responsabile della Protezione dei Dati, valuta se contattare il Garante per chiedere suggerimenti sulla necessità di comunicare l'incidente agli interessati e sull'individuazione del messaggio più appropriato da fornire.

Lo strumento per effettuare tale comunicazione varia in base al numero dei soggetti interessati da contattare, al

costo e ai mezzi normalmente utilizzati per le comunicazioni con i soggetti interessati.

La comunicazione è individuale e compiuta per iscritto (via e-mail, tramite sms, etc...). Tuttavia, ove ciò richiedesse degli sforzi sproporzionati, è possibile procedere anche con una comunicazione pubblica (*banner* o *post* su sito internet, pubblicazione di annuncio sul giornale, etc...). In ogni caso, la comunicazione deve essere trasparente ed effettuata con mezzi tali da garantire che gli interessati siano effettivamente informati del fatto che si è verificato un *Personal Data Breach*.

La comunicazione dovrà contenere:

- una breve descrizione dell'accaduto, data (o date) della violazione e della relativa scoperta e descrizione del tipo di Informazioni Personali che sono state compromesse;
- potenziale rischio causato dalla violazione e entità del danno;
- azioni che gli Interessati ed il Comune dovranno intraprendere per limitare l'entità del danno;
- la descrizione delle misure già adottate dal Comune per porre rimedio al *Personal Data Breach* e per attenuarne le conseguenze nonché quelle che sono state e verranno adottate per evitare eventuali future violazioni;
- il nominativo e i recapiti (numero di telefono, indirizzi e-mail) del Responsabile della protezione dei dati o dei Designati per il trattamento dei dati da contattare per ottenere maggiori informazioni.

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

- il Titolare del trattamento ha messo in atto misure di sicurezza tecniche e organizzative adeguate e tali misure sono state applicate ai dati personali oggetto della violazione. In particolare, rilevano le misure di sicurezza che rendono i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali per esempio la cifratura;
- il Titolare del trattamento ha adottato successivamente all'incidente misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece alla pubblicazione di un avviso pubblico o all'adozione di altre misure simili, tramite le quali gli interessati sono informati con analoga efficacia.

E. Registro dei *Personal Data Breach*

È istituito un registro in cui il Responsabile della protezione dei dati dovrà documentare gli incidenti di sicurezza/*Personal Data Breach* a prescindere dal fatto che da questi sia seguita la notifica al Garante e/o la comunicazione agli Interessati.
Il registro deve contenere (i) la descrizione della tipologia di dati oggetto della violazione, (ii) le cause, (iii) gli effetti, (iv) le azioni poste in essere per rimediarvi, (v) le motivazioni per le quali si è deciso di non procedere alla notifica al Garante e/o alla comunicazione agli Interessati ovvero l'indicazione della notifica effettuata e delle eventuali successive integrazioni.
Dovranno essere altresì documentate le ragioni che hanno condotto alla Notifica per fasi o al ritardo nella notifica.
Il registro dovrà inoltre indicare se, a seguito di un *Personal Data Breach*, è stata effettuata la comunicazione al soggetto interessato, i relativi tempi e mezzi di comunicazione utilizzati.
Il registro è tenuto dal Responsabile della protezione dei dati .

F. Calcolo del livello di rischio

Per effettuare la predetta valutazione, vengono utilizzati i criteri di seguito elencati, tenendo conto della probabilità di accadimento del danno e della gravità delle conseguenze. Tali criteri rappresentano una mera esemplificazione, fermo restando che la valutazione andrà condotta sul caso specifico e con riguardo al contesto di riferimento.

Tipologia di *Data Breach*	Viene valutato se è relativo alla confidenzialità, disponibilità e/o integrità dei dati. Si consideri che una violazione concernente la confidenzialità dei dati riguardanti la carriera di uno studente può avere un livello di rischio e un impatto diverso (e minore) rispetto alla perdita o distruzione definitiva dei predetti dati.
Natura, tipologia e sensibilità dei dati violati	Generalmente, maggiore è la sensibilità dei dati violati maggiore è il rischio di lesione dei diritti e delle libertà degli individui (per esempio, la violazione della confidenzialità dei dati sulla salute ha delle conseguenze più gravi della violazione della confidenzialità dei dati anagrafici di un soggetto).
Facilità d'identificazione diretta o indiretta dei soggetti interessati	Ove l'incidente riguardi dati che non permettono la diretta identificazione degli Interessati, il livello di rischio è minore (per es. la violazione di dati criptati o de identificati è sicuramente meno grave della violazione di dati in chiaro o accompagnati dagli identificativi diretti degli Interessati).
Gravità delle conseguenze per i soggetti interessati	Ad esempio, il rischio dovrà essere valutato elevato ove dalla violazione possa derivare un furto di identità, un danno materiale, un danno di immagine. Analogamente, deve considerarsi elevato il rischio qualora siano stati violati i diritti e le libertà fondamentali dei soggetti interessati quando il Titolare è consapevole che i dati personali sono stati violati e si ritiene che il soggetto che li detiene abbia intenzioni sospette o malevoli.
Categorie dei soggetti interessati	In caso di violazione di Informazioni Personali concernenti minori o soggetti vulnerabili (ad esempio soggetti con disabilità etc...) il rischio si considera più elevato.
Numero di soggetti coinvolti	Generalmente, maggiore è il numero di soggetti interessati, più elevato è il rischio.

Il rischio (R) è calcolato mediante la seguente formula:

R = Probabilità della minaccia X Impatto

Il rischio è tanto maggiore quanto più è probabile che accada l'incidente e tanto maggiore è la gravità del danno arrecato (impatto). Una volta determinati gli indici di rischio sarà possibile individuarne la significatività e definire quindi le priorità d'intervento. In base ai valori attribuibili alle due variabili "Probabilità della Minaccia" e "Impatto", il rischio è numericamente definito con una scala crescente dal valore 1 al valore 12 secondo la matrice riportata nella seguente tabella

	IMPATTO			
PROBABILITÀ DELLA MINACCIA	Basso (1)	Medio (2)	Elevato (3)	Molto Elevato (4)
Basso (1)	1	2	3	4
Medio (2)	2	4	6	8
Alto (3)	3	6	9	12

La probabilità è misurata mediante la ponderazione delle variabili che influenzano il trattamento del dato come: le risorse tecniche utilizzate, i processi e le procedure e la tipologia di trattamento svolto. Per maggiori dettagli si rinvia al documento dell'ENISA denominato "*Guidelines for SMEs on the security of personal data processing*" del dicembre 2016, pagg. da 24 a 30.

L'impatto della violazione viene misurato in base ai soggetti coinvolti nel trattamento.

LIVELLI DI IMPATTO

Nullo/Basso	I soggetti interessati non vengono colpiti o subirebbero disagi minimi, superabili senza alcun problema (tempo necessario per reinserire le informazioni, fastidio, irritazione etc…)
Medio	I soggetti interessati subiscono notevoli disagi risolvibili con qualche difficoltà (costi extra, negazione accesso a servizi aziendali, timori, difficoltà di comprensione, stress, indisposizione fisica, etc...)
Elevato	I soggetti interessati subiscono notevoli disagi risolvibili con serie difficoltà (appropriazione indebita di fondi, inserimento nella *black list* dei cattivi pagatori da parte delle banche, danni a proprietà, perdita dell'impiego, citazione a comparire, peggioramento dello stato di salute, etc…)
Molto Elevato	I soggetti interessati subiscono notevoli conseguenze, perfino irreversibili, e impossibili da risolvere (difficoltà finanziarie quali ingenti debiti, impossibilità a lavorare, problemi fisici o psicologici a lungo termine, morte, etc...)

G. Violazioni della presente procedura

La violazione di quanto previsto nella presente *Policy* espone il Titolare del trattamento al rischio di responsabilità civile, penale e a sanzioni amministrative. Il soggetto autore delle violazioni potrà incorrere in responsabilità disciplinare e conseguentemente nei provvedimenti sanzionatori, secondo quanto previsto dalla normativa vigente e dal CCNL di riferimento applicabile.

Allegato B)

Esempi di *Data Breach* e comunicazioni

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un titolare del trattamento ha memorizzato un backup di archivio dati personali criptati su una chiavetta USB. La chiavetta UBS viene rubata durante un furto con scasso.	No.	No.	Fintanto che i dati sono criptati con un algoritmo di ultima generazione, che esistono dei *backup* dei dati che possono essere recuperati in tempi rapidi, e che la chiave univoca non sia stata compromessa, non si tratta di una violazione da notificare. Tuttavia, se successivamente compromessa, la violazione va notificata.
Un titolare del trattamento offre un servizio online. Durante un attacco informatico a tale servizio vengono prelevati dei dati personali di individui. Il titolare del trattamento ha clienti in un singolo Stato membro.	Sì. Notificare l'autorità di controllo competente in presenza di potenziali conseguenze per singoli individui.	Sì. Notificare gli individui a seconda della natura dei dati personali interessati, e nel caso in cui vi siano alte potenziali conseguenze per gli individui.	Se il rischio non è elevato, è consigliabile che il titolare del trattamento informi la persona interessata, a seconda delle circostanze del caso. Potrebbe ad esempio non essere necessario informare nel caso di violazione di una newsletter relativa a un programma televisivo, tuttavia la notifica potrebbe essere necessaria se la newsletter può influenzare il punto di vista politico sull'argomento trattato.

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Una breve interruzione di corrente elettrica della durata di qualche minuto presso il call center del titolare del trattamento non ha consentito ai clienti né di chiamare il titolare del trattamento né di accedere ai propri archivi.	No.	No.	Non si tratta di una violazione di dati personali notificabile, sebbene si tratti comunque di un incidente registrabile ai sensi dell'articolo 33. Il titolare del trattamento deve assicurare la registrazione del caso.
Un titolare del trattamento viene fatto oggetto di un attacco con richiesta di riscatto in seguito al quale tutti i dati vengono criptati. Non sono disponibili *backup* e non è possibile ripristinare i dati. In seguito ad accertamenti emerge con certezza che l'unico scopo dell'attacco era quello di criptare i dati, e che non vi è alcun altro *malware* presente nel sistema.	Sì. Notificare l'autorità di controllo competente se vi sono potenziali conseguenze per le persone poiché ciò rappresenta una mancanza di disponibilità.	Sì. Notificare i soggetti a seconda della natura dei dati personali interessati, del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Nel caso vi sia un *backup* disponibile e i dati possano essere ripristinati in breve tempo, non è necessario segnalare l'evento all'autorità di controllo o alle persone, in quanto non vi si configura una mancanza permanente di disponibilità né di riservatezza. Tuttavia, le autorità di controllo potrebbe ritenere necessaria un'indagine per valutare la conformità con i requisiti di sicurezza generali di cui all'art. 32.

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Una persona chiama il call center di una banca segnalando una violazione di dati. Questo individuo ha ricevuto l'estratto conto mensile di qualcun altro. Il titolare del trattamento svolge una breve indagine (entro le 24 ore) e stabilisce con ragionevole certezza che vi è stata una violazione di dati personali, e se si tratti di un difetto sistemico che potrebbe compromettere anche altri soggetti.	Si.	Vanno notificate soltanto le persone interessate, se vi è un alto rischio e se risulta evidente che non siano stati coinvolti altri.	Se in seguito a ulteriori indagini emerge che sono interessati anche altri individui, è necessario un aggiornamento all'autorità di controllo e il titolare del trattamento dovrà notificare altri soggetti nel caso in cui vi sia per essi un rischio elevato.
Una multinazionale del commercio online viene fatta oggetto di un attacco informatico in seguito al quale vengono pubblicati in rete nomi utente, *password* e storia degli acquisti.	Sì. Segnalare il problema all'autorità centrale di controllo in presenza di dati transfrontalieri.	Sì, in quanto ciò potrebbe causare alti livelli di rischio.	Il titolare del trattamento deve intervenire, ad esempio forzando il ripristino delle *password* dei conti interessati, oppure seguire altri *step* per ridurre il rischio.

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un'azienda di *web hosting* (un responsabile del trattamento) identifica un errore nel codice che controlla l'autorizzazione utenti. Il risultato è che ogni utente può accedere ai dettagli dell'*account* di qualsiasi altro utente.	Come responsabile del trattamento l'azienda di web hosting deve immediatamente notificare i propri clienti (i titolari del trattamento) interessati. Dato per scontato che l'azienda di web hosting abbia condotto una propria indagine, i titolari del trattamento interessati devono essere ragionevolmente sicuri se abbiano o meno subito una violazione e, pertanto, se possano ritenersi "a conoscenza" una volta informati dall'azienda di *web hosting* (responsabile del trattamento). A questo punto il titolare del trattamento deve informare l'autorità di controllo.	Se è probabile che non vi sia un elevato rischio per le persone, queste non devono essere notificate.	L'azienda di *web hosting* (responsabile del trattamento) deve tenere in considerazione eventuali altri obblighi di notifica, ad es. in base alla Direttiva di sicurezza delle reti e dei sistemi informativi (NIS). Se non vi è alcuna evidenza che questa vulnerabilità venga sfruttata dal titolare del trattamento, una violazione notificabile potrebbe non essersi verificata. Tuttavia è probabile che sia registrabile ovvero che configuri una non conformità ai sensi dell'art. 32.
A causa di un attacco informatico in un ospedale le cartelle cliniche non sono disponibili per un arco di 30 ore.	Sì. L'ospedale è tenuto a segnalare un potenziale elevato rischio per il benessere e la *privacy* dei pazienti.	Sì. Notificare i soggetti colpiti.	
I dati personali di 5.000 studenti vengono erroneamente inviati a una *mailing list* che include oltre 1.000 persone.	Sì, notificare l'autorità di controllo.	Sì, notificare gli individui a seconda della portata e della tipologia di dati personali coinvolti e della gravità delle possibili conseguenze.	

Caso	Notificare l'autorità di controllo?	Notificare la persona interessata?	Note/raccomandazioni
Un'e-mail di *direct marketing* viene inviata ai destinatari nei campi "To:" o "Cc:" permettendo così a ciascun destinatario di visualizzare l'indirizzo di posta elettronica degli altri destinatari.	Sì. Potrebbe essere obbligatorio notificare l'autorità di controllo se è interessato un alto numero di individui, nel caso in cui siano rivelati dati sensibili (ad es. una *mailing list* di uno psicoterapeuta) oppure nel caso in cui altri fattori presentino rischi elevati (ad es. il messaggio e-mail contiene le *password* iniziali)	Sì, notificare gli individui a seconda della portata e della tipologia di dati personali coinvolti e della gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non sono stati rivelati dati sensibili e se sia stato rivelato solo un numero ridotto di indirizzi di posta elettronica.

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

Il presidente	Il segretario comunale
ENNIO VALIANTE	DANIELA GIACOMIN

Documento informatico sottoscritto con firma elettronica ai sensi e con gli effetti di cui agli artt. 20 e 21 del d.lgs. 7.03.2005, n.82 e ss. mm.; sostituisce il documento cartaceo e la firma autografa.