



COMUNE DI PONTENURE

PROVINCIA DI PIACENZA

Pontenure, 09.09.2026

DIRETTIVA N. 4/2026

IL SEGRETARIO GENERALE

Ai Responsabili di Settore/Servizio

A tutti i dipendenti comunali

Al Sindaco

Alla Giunta Comunale

**Al Responsabile della Protezione dei
dati**

Al OIV

OGGETTO: Protezione dei dati personali nell'attività amministrativa – Indicazioni operative per gli uffici comunali e gli organi politici – Obblighi di riservatezza, pubblicazione, accesso e diffusione dei dati personali.

1. Premessa

La protezione dei dati personali costituisce un obbligo trasversale che interessa ogni attività dell'Amministrazione comunale e coinvolge non soltanto gli uffici e il personale dipendente, ma anche gli organi politici nell'esercizio delle rispettive funzioni.

Il tema assume particolare rilievo in considerazione della crescente quantità di dati personali trattati dall'Amministrazione attraverso procedimenti amministrativi, sistemi informatici, pubblicazioni sul sito istituzionale, Albo pretorio, Amministrazione trasparente, posta elettronica, sistemi di videosorveglianza e canali di comunicazione istituzionale.

La presente direttiva prende le mosse dalle criticità evidenziate nel documento “**Direttiva Privacy – Aggiornamenti operativi**” del 14 luglio 2026, relativo alla Relazione annuale del Garante per la protezione dei dati personali sulle attività svolte nel 2025, con particolare riferimento ai trattamenti effettuati dagli enti pubblici e dagli enti locali.

Dall'esame delle fattispecie richiamate emerge l'esigenza di rafforzare, all'interno dell'Ente, una cultura amministrativa improntata ai principi di **liceità, correttezza, trasparenza, minimizzazione e proporzionalità del trattamento**, evitando che gli obblighi di pubblicità e trasparenza dell'azione amministrativa si traducano in un'indiscriminata diffusione di dati personali.

Il quadro nazionale di riferimento è costituito, in particolare, dal **D.Lgs. 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali**, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679. L'art. 2-ter del Codice disciplina la base giuridica del trattamento effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

2. Principio generale: non tutto ciò che è detenuto dall'Amministrazione può essere pubblicato

Si richiama l'attenzione di tutti i destinatari della presente direttiva sul principio secondo cui **la mera disponibilità di un dato personale da parte del Comune non costituisce, di per sé, titolo sufficiente per la sua pubblicazione o diffusione.**

Prima di procedere alla pubblicazione di un atto o documento occorre pertanto verificare:

1. quale sia la finalità della pubblicazione;
2. quale sia la specifica disposizione normativa che ne impone o consente la pubblicazione;
3. quali dati personali siano effettivamente necessari rispetto alla finalità perseguita;
4. se sia possibile raggiungere la medesima finalità mediante l'omissione o l'oscuramento dei dati personali non necessari;
5. se il documento contenga categorie particolari di dati personali o dati relativi a condanne penali e reati;
6. quale sia il periodo di pubblicazione previsto dalla normativa applicabile.

L'art. 2-ter del D.Lgs. n. 196/2003 individua la base giuridica del trattamento dei dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Ne consegue che **la pubblicazione deve sempre essere preceduta da una specifica verifica di liceità e di necessità.**

3. Deliberazioni, determinazioni e altri atti amministrativi

I Responsabili di Settore sono tenuti, nella predisposizione degli atti destinati alla pubblicazione, ad applicare il principio di minimizzazione.

In particolare:

- devono essere inseriti negli atti esclusivamente i dati personali pertinenti e necessari alla motivazione e alla decisione amministrativa;
- devono essere evitati dati personali eccedenti rispetto alla finalità dell'atto;
- devono essere attentamente verificati gli allegati, che sono parte integrante dell'atto e sono pertanto soggetti alla medesima attenzione sotto il profilo della protezione dei dati;
- i dati relativi alla salute, alla disabilità, a situazioni personali particolarmente delicate, a procedimenti penali o ad altre categorie particolari di dati devono essere trattati con particolare cautela;

- quando la pubblicazione dell'atto è obbligatoria, deve essere pubblicata esclusivamente la parte necessaria al perseguimento della finalità di pubblicità prevista dalla legge.

Particolare attenzione dovrà essere prestata alle **deliberazioni della Giunta e del Consiglio comunale**, soprattutto quando riguardino contenzioso, personale, procedimenti disciplinari, situazioni sociali, disabilità, salute o altre vicende personali.

La pubblicazione di dati personali non necessari non può essere giustificata dalla sola esigenza di assicurare una maggiore trasparenza dell'attività amministrativa.

4. Albo pretorio e Amministrazione trasparente

Si richiama espressamente l'attenzione dei Responsabili sulla necessità di distinguere:

- l'obbligo di pubblicazione all'Albo pretorio;
- gli obblighi di pubblicazione nella sezione “Amministrazione trasparente”;
- la mera disponibilità del documento agli interessati mediante accesso agli atti.

Le tre fattispecie non sono equivalenti e non consentono automaticamente la medesima forma di diffusione dei dati.

Il documento esaminato evidenzia numerosi casi nei quali enti locali hanno pubblicato online dati personali eccedenti, tra cui nominativi, dati relativi a contenziosi, informazioni concernenti la salute, vicende personali dei dipendenti, dati contenuti nelle dichiarazioni di inconferibilità e incompatibilità e altri elementi non necessari alla finalità di pubblicità.

Pertanto, **prima della pubblicazione dovrà essere effettuato un controllo specifico anche degli allegati.**

5. Registro degli accessi

Particolare attenzione deve essere prestata alla gestione e all'eventuale pubblicazione del registro degli accessi.

Il documento allegato richiama il caso di alcuni enti locali che avevano pubblicato online registri contenenti migliaia di richieste di accesso, con nomi e cognomi dei richiedenti e dei destinatari, numeri di protocollo, oggetto e descrizione delle istanze e, in alcuni casi, informazioni relative a proprietari di immobili, pratiche edilizie e persino informazioni sullo stato di salute di cittadini.

Il registro eventualmente pubblicato **non deve pertanto contenere dati identificativi dei richiedenti, dei controinteressati o di altri soggetti quando tali dati non siano necessari alla finalità di trasparenza perseguita.**

Prima della pubblicazione dovrà essere effettuata un'adeguata attività di oscuramento.

6. Contenzioso e atti relativi a procedimenti giudiziari

Particolare cautela dovrà essere adottata nella pubblicazione di deliberazioni e determinazioni relative a:

- costituzione o resistenza in giudizio;
- conferimento di incarichi legali;
- transazioni;
- controversie giudiziarie;
- procedimenti amministrativi connessi a contenziosi.

Il documento allegato richiama il caso di deliberazioni comunali i cui allegati riportavano nominativi delle parti, date di nascita, indirizzi di residenza e codici fiscali.

La pubblicazione online di tali dati è risultata sproporzionata rispetto alla finalità di pubblicità dell'atto.

Pertanto, negli atti destinati alla pubblicazione dovranno essere inseriti esclusivamente gli elementi necessari alla comprensione della decisione amministrativa, procedendo all'oscuramento dei dati personali non necessari.

7. Dati relativi alla salute, disabilità e altre categorie particolari

È fatto divieto di inserire negli atti destinati alla pubblicazione dati relativi alla salute o altre informazioni particolarmente delicate quando tali informazioni non siano strettamente necessarie e giuridicamente giustificate.

Il D.Lgs. n. 196/2003 dedica specifiche disposizioni alle categorie particolari di dati. L'art. 2-sexies disciplina il trattamento delle categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante, richiedendo che siano individuati, secondo le condizioni previste dalla norma, i tipi di dati trattabili, le operazioni eseguibili e le garanzie appropriate e specifiche per la tutela degli interessati.

L'art. 2-septies disciplina inoltre le misure di garanzia relative al trattamento dei dati genetici, biometrici e relativi alla salute.

Ne consegue che informazioni quali:

- diagnosi;
- percentuali di invalidità;
- certificazioni sanitarie;
- riferimenti a malattie o condizioni di salute;
- fruizione di congedi o istituti collegati a condizioni personali o familiari;
- informazioni relative a disabilità;

non devono essere riportate negli atti pubblicati online se non nei limiti strettamente necessari e consentiti dalla normativa.

8. Procedimenti penali e dati relativi a reati

Analoga attenzione deve essere prestata ai dati relativi a procedimenti penali, condanne e reati.

Il D.Lgs. n. 196/2003 disciplina specificamente tali trattamenti all'art. 2-octies, prevedendo specifiche condizioni per il trattamento dei dati relativi a condanne penali e reati.

Pertanto, nei verbali, nelle deliberazioni, nelle determinazioni, nei documenti relativi a procedure concorsuali e negli altri atti destinati alla pubblicazione dovrà essere evitata la diffusione di tali informazioni quando non espressamente prevista e necessaria sulla base di una specifica disposizione normativa.

9. Accesso agli atti e accesso civico

La disciplina della protezione dei dati personali **non può essere utilizzata automaticamente per negare ogni forma di accesso.**

Ogni richiesta deve essere esaminata concretamente, verificando la specifica disciplina applicabile e valutando, ove possibile, l'accesso parziale mediante oscuramento dei dati personali non necessari.

Il documento allegato richiama, infatti, numerosi casi nei quali il Garante ha ritenuto possibile consentire l'accesso attraverso l'oscuramento dei dati identificativi, dei dati di contatto, delle firme e delle altre informazioni eccedenti rispetto alla finalità conoscitiva.

Pertanto, gli uffici dovranno privilegiare, ove giuridicamente possibile, la soluzione dell'**ostensione parziale con oscuramento dei dati personali eccedenti**, anziché procedere automaticamente al diniego integrale.

10. Posta elettronica e comunicazioni agli interessati

Nell'utilizzo della posta elettronica istituzionale dovrà essere prestata particolare attenzione ai destinatari delle comunicazioni.

È fatto obbligo di:

- verificare sempre i destinatari prima dell'invio;
- utilizzare il campo "CCN" quando una comunicazione è indirizzata a più soggetti che non devono conoscere gli indirizzi degli altri destinatari;
- evitare l'invio in chiaro di elenchi di indirizzi e-mail;
- non inserire nell'oggetto delle e-mail informazioni personali eccedenti o dati particolari;
- prestare particolare attenzione alle comunicazioni riguardanti minori, disabilità, salute, procedimenti disciplinari o altre situazioni personali.

Il documento allegato richiama espressamente il caso di una comunicazione inviata mediante mailing list in chiaro, attraverso la quale erano stati resi conoscibili a più destinatari indirizzi e-mail e informazioni relative allo stato vaccinale di minori.

11. Sito istituzionale e social network dell'Ente

La pubblicazione di fotografie, filmati e altri contenuti sulle pagine istituzionali dell'Ente, compresi i social network, deve essere preceduta da una verifica della relativa base giuridica.

La circostanza che un'immagine sia stata acquisita durante un'iniziativa organizzata o patrocinata dal Comune **non comporta automaticamente la possibilità di pubblicarla**.

Particolare cautela deve essere adottata per:

- minori;
- persone con disabilità;
- utenti di servizi sociali o educativi;
- soggetti coinvolti in procedimenti amministrativi;
- dipendenti;
- persone che si trovino in situazioni personali delicate.

Il documento allegato richiama un caso nel quale un Comune era stato sanzionato per la pubblicazione su Facebook di fotografie e video riguardanti minori e persone con disabilità, evidenziando inoltre che, per i soggetti pubblici, il consenso non costituisce automaticamente la base giuridica idonea per i trattamenti effettuati nell'esercizio delle funzioni istituzionali.

Prima della pubblicazione di immagini dovrà quindi essere verificata la **specificità finalità istituzionale, la base giuridica e la necessità della diffusione**.

12. Videosorveglianza

Particolare attenzione dovrà essere assicurata alla gestione dei sistemi di videosorveglianza comunale.

Ogni sistema dovrà essere utilizzato esclusivamente per le finalità per le quali è stato legittimamente installato.

Non è consentito utilizzare le immagini raccolte per una finalità diversa da quella originariamente individuata in assenza di un'idonea base giuridica.

Dovranno inoltre essere verificati:

- la corretta informativa di primo livello mediante cartellonistica;
- la presenza e l'accessibilità dell'informativa di secondo livello;
- la corretta individuazione delle finalità;
- la configurazione tecnica del sistema;
- i tempi di conservazione;
- l'accesso alle immagini;
- le eventuali ulteriori garanzie richieste dalla normativa.

Il documento allegato richiama specificamente casi nei quali comuni sono stati sanzionati per carenze nella cartellonistica e nell'informativa, nonché per l'utilizzo delle immagini raccolte per finalità ulteriori rispetto a quelle originariamente previste.

Qualora il sistema possa consentire il controllo a distanza dell'attività dei lavoratori, dovrà inoltre essere verificato preventivamente il rispetto dell'art. 4 della **Legge 20 maggio 1970, n. 300**, che disciplina gli impianti audiovisivi e gli altri strumenti dai quali possa derivare anche la possibilità di controllo a distanza dei lavoratori.

13. Trattamento dei dati dei dipendenti

Nella gestione del rapporto di lavoro dovrà essere assicurato il rispetto del principio di necessità e pertinenza dei dati trattati.

Non devono essere raccolti o utilizzati dati ulteriori rispetto a quelli necessari per la gestione del rapporto di lavoro e per le finalità istituzionali previste dalla normativa.

Particolare attenzione dovrà essere prestata all'utilizzo di strumenti tecnologici che consentano il monitoraggio dei dipendenti.

Il documento allegato richiama il caso di un sistema di geolocalizzazione dei lavoratori in smart working attraverso il quale venivano raccolte informazioni sulla posizione geografica dei dipendenti. L'Autorità ha ritenuto tale modalità non conforme, evidenziando che la sicurezza dei dati deve essere assicurata attraverso adeguate misure tecniche e organizzative e specifiche istruzioni agli autorizzati, e non attraverso forme di controllo non consentite.

Il D.Lgs. n. 196/2003, all'art. 2-quaterdecies, prevede che il titolare o il responsabile possano attribuire specifici compiti e funzioni connessi al trattamento a persone fisiche espressamente designate, individuando le modalità più opportune per autorizzarle al trattamento.

14. Procedure concorsuali e selettive

Negli atti relativi a concorsi e selezioni dovrà essere verificata con particolare attenzione la possibilità di pubblicare i verbali delle commissioni e gli altri documenti contenenti dati personali dei candidati.

Il documento allegato richiama un caso nel quale erano stati pubblicati sul sito istituzionale verbali contenenti dati personali dei partecipanti, comprese dichiarazioni relative a procedimenti penali, successivamente indicizzati dai motori di ricerca.

Pertanto, **non dovranno essere pubblicati automaticamente tutti gli atti formati nell'ambito di una procedura concorsuale**, ma esclusivamente quelli per i quali sussista uno specifico obbligo di pubblicazione, nei limiti dei dati necessari.

15. Whistleblowing

Per la gestione delle segnalazioni di whistleblowing dovrà essere assicurato il massimo livello di riservatezza dell'identità del segnalante e delle altre persone coinvolte.

Particolare attenzione dovrà essere prestata:

- al canale utilizzato per la segnalazione;
- alla sicurezza delle comunicazioni;
- alla gestione degli accessi;
- ai tempi di conservazione;
- alla separazione delle competenze;

- alla prevenzione di accessi non autorizzati;
- alla protezione dei dati delle persone coinvolte.

Il documento allegato evidenzia, in particolare, i rischi connessi all'utilizzo della posta elettronica come canale di segnalazione, la necessità di valutare preventivamente gli impatti sul trattamento dei dati, i tempi di conservazione e l'adozione di adeguate misure tecniche e organizzative.

16. Indicazioni specifiche per gli organi politici

Gli amministratori comunali, nell'esercizio delle proprie funzioni, sono tenuti a prestare particolare attenzione alla riservatezza delle informazioni e dei documenti acquisiti per ragioni istituzionali.

In particolare, **documenti, dati e informazioni acquisiti nell'ambito dell'attività istituzionale non devono essere diffusi o comunicati a soggetti estranei quando tale comunicazione non sia consentita dalla normativa.**

Particolare cautela deve essere adottata nella:

- pubblicazione di documenti sui social network personali;
- trasmissione di documenti mediante sistemi di messaggistica;
- condivisione di documenti contenenti dati personali in gruppi o chat;
- divulgazione di informazioni relative a procedimenti amministrativi ancora in corso;
- diffusione di informazioni relative a cittadini, dipendenti, minori, persone con disabilità o soggetti coinvolti in procedimenti giudiziari.

Il fatto che un amministratore abbia avuto accesso legittimamente a un documento **non comporta automaticamente la possibilità di divulgarne il contenuto.**

17. Obbligo di verifica preventiva da parte dei Responsabili

A decorrere dalla data della presente circolare, i Responsabili di Settore/Servizio sono invitati a prevedere, nell'ambito dei propri procedimenti, una specifica verifica preventiva degli atti destinati alla pubblicazione.

In particolare, prima della pubblicazione dovrà essere verificato:

- a) se esiste uno specifico obbligo normativo di pubblicazione;
- b) quali dati devono essere necessariamente pubblicati;
- c) quali dati possono essere omessi;
- d) se sono presenti dati relativi alla salute, disabilità, procedimenti penali o altre categorie particolari;
- e) se gli allegati contengono dati personali eccedenti;
- f) se sia necessario procedere all'oscuramento di parti del documento;
- g) la durata della pubblicazione;
- h) l'eventuale necessità di coinvolgere il Responsabile della Protezione dei Dati.

La verifica dovrà essere effettuata **prima della trasmissione dell'atto per la pubblicazione**, e non successivamente alla pubblicazione.

18. Obbligo di segnalazione di eventuali violazioni

Qualsiasi dipendente o Responsabile che venga a conoscenza di un possibile incidente relativo ai dati personali dovrà darne **tempestiva comunicazione secondo le procedure interne dell'Ente al RPD/DPO**, senza procedere autonomamente alla cancellazione o alla modifica delle evidenze necessarie per ricostruire l'accaduto.

Rientrano, a titolo esemplificativo:

- invio di una e-mail a destinatario errato;
- perdita o furto di documentazione;
- accesso non autorizzato a sistemi informatici;
- pubblicazione online di dati non dovuti;
- invio di documenti a soggetti non autorizzati;
- smarrimento di dispositivi contenenti dati personali;
- divulgazione accidentale di informazioni personali.

La tempestività della segnalazione è essenziale per consentire all'Ente di valutare l'eventuale violazione dei dati personali e gli adempimenti conseguenti.

19. Ruolo dei Responsabili e dei soggetti autorizzati

I Responsabili di Settore sono chiamati a garantire, nell'ambito delle rispettive strutture, il rispetto delle disposizioni in materia di protezione dei dati personali e a impartire al personale le necessarie istruzioni operative.

Il personale autorizzato al trattamento è tenuto a:

- trattare i dati esclusivamente per le finalità istituzionali;
- accedere esclusivamente ai dati necessari allo svolgimento delle proprie funzioni;
- non comunicare dati a soggetti non autorizzati;
- mantenere la riservatezza sulle informazioni acquisite per ragioni di servizio;
- utilizzare correttamente gli strumenti informatici;
- adottare ogni cautela necessaria per impedire accessi non autorizzati;
- segnalare tempestivamente eventuali incidenti o anomalie.

20. Indicazioni finali

La protezione dei dati personali deve essere considerata parte integrante della corretta gestione amministrativa.

La trasparenza dell'azione amministrativa e la tutela della riservatezza **non costituiscono principi necessariamente contrapposti**, ma devono essere concretamente bilanciati attraverso una corretta individuazione della base giuridica, della finalità del trattamento e dei dati effettivamente necessari.

Alla luce delle criticità evidenziate nel documento allegato, si richiama pertanto l'attenzione di tutti i destinatari affinché:

1. nessun documento venga pubblicato automaticamente nella sua integralità senza una preventiva verifica;
2. siano sempre verificati anche gli allegati agli atti;
3. siano oscurati i dati personali eccedenti rispetto alla finalità di pubblicazione;
4. sia prestata particolare attenzione ai dati relativi alla salute, alla disabilità, ai minori e ai procedimenti penali;
5. le richieste di accesso siano esaminate secondo la disciplina specificamente applicabile, valutando ove possibile l'accesso parziale mediante oscuramento;
6. la pubblicazione di immagini e video sui canali istituzionali sia preceduta dalla verifica della relativa base giuridica;
7. i sistemi di videosorveglianza siano utilizzati esclusivamente per finalità previamente individuate e nel rispetto delle garanzie previste;
8. siano evitati strumenti tecnologici che determinino forme di controllo dei lavoratori non consentite dalla normativa;
9. ogni possibile violazione dei dati personali sia segnalata tempestivamente secondo le procedure dell'Ente;
10. per le questioni di particolare complessità o in presenza di dubbi sulla liceità di un trattamento venga preventivamente coinvolto il Responsabile della Protezione dei Dati.

Infine, per ogni opportuno approfondimento, si demanda alle *"Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"* del Garante Privacy qui reperibili <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3134436>.

La presente direttiva deve essere portata a conoscenza di tutto il personale dell'Ente e costituisce **direttiva organizzativa interna per le attività di competenza dei Responsabili di Settore/Servizio**.

Si confida nella piena collaborazione di tutti i destinatari, al fine di assicurare che l'attività amministrativa dell'Ente sia svolta nel pieno rispetto dei principi di legalità, trasparenza, proporzionalità e tutela della dignità e della riservatezza delle persone.

IL SEGRETARIO GENERALE

Dott. Francesco Palopoli
(firmato digitalmente)

FRANCESCO
PALOPOLI
09.09.2026
11:48:36
GMT+01:00

