Ill.mi
Sindaco
Segretario comunale RPCT

COMUNE DI MONTALE (PT)
via PEC: comune.montale@postacert.toscana.it

Oggetto: Trattamento dati whistleblowing D.Lgs. 10 marzo 2023, n. 24 – Valutazione d'impatto ex art. 35, GDPR – Parere ex art. 39, c. 1, lett. c), GDPR

Si rende il richiesto parere in oggetto, nei termini seguenti.

Si dà atto che la valutazione d'impatto in oggetto, come da ultimo inviatami in data 23 aprile 2026, è definita utilizzando la metodologia messa a disposizione dall'Autorità Garante per la Protezione Dati Personali attraverso il software PIA.

L'art. 13, c.6, del D.Lgs. 10 marzo 2023 n.24, stabilisce quanto segue: «*I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018.*».

La base giuridica del trattamento per le finalità indicate è stabilita dal decreto sopra citato, richiamato dalla valutazione d'impatto in esame. Il trattamento è dunque legittimo in relazione alle predette finalità.

La valutazione d'impatto dimostra che il trattamento risulta pertinente e limitato rispetto alle finalità, definito nel rispetto del principio privacy by design tenuto conto delle modalità implementate; emerge inoltre che il trattamento non determina la raccolta e l'estrapolazione di dati se non quelli strettamente necessari per la finalità (minimizzazione).

Posto che il trattamento è effettuato mediante il ricorso a piattaforma gestita da responsabile esterno, l'adeguatezza delle misure di sicurezza dallo stesso definite ed attuate risulta determinante per una positiva valutazione, adeguatezza da verificare periodicamente da parte del Titolare. L'importanza di tali aspetti si ricava anche dal sopra riportato sesto comma, che cita espressamente la figura del responsabile esterno e la necessità di disciplinare il rapporto con quest'ultimo.

La difesa dei sistemi (intesa come difesa del dato in trattamento) definita dalle misure di sicurezza previste, viene considerata dalla valutazione d'impatto adeguata rispetto al trattamento dei dati,

determinando una stima del rischio residuo accettabile nelle sue diverse dimensioni di integrità, disponibilità e riservatezza. La valutazione tecnica del rischio, nei termini di impatto per la libertà ed incolumità della persona a cui sono riferiti i dati personali, prende in esame oltre ai classici rapporti di probabilità e gravità, anche la capacità di resilienza nel mitigare il rischio per contrastare l'avversità opponente rappresentata da eventuali inservibilità od esfiltrazioni indebite dei dati.

Viene indicato che sono messe a disposizione informazioni sulle procedure per effettuare le segnalazioni, in conformità all'art. 5 del citato D.Lgs. n.24/2023.

In merito al periodo di conservazione l'allegato tecnico del sistema utilizzato prevede una "Policy di data retention di default delle segnalazioni di 12 mesi, con cancellazione automatica sicura delle segnalazioni che raggiungono la data di scadenza", con la possibilità del gestore di "prorogare la scadenza delle segnalazioni per il tempo ritenuto congruo al trattamento dei dati". L'art.14, c.1, del D.Lgs. n.24/2023, stabilisce che "Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione". Si rileva, pertanto, che il periodo "necessario al trattamento della segnalazione" di cui al riportato art.14, potrebbe risultare superiore a quello "di 12 mesi" al termine del quale il sistema dispone la cancellazione automatica, richiedendo, quindi, un apposito intervento di proroga da parte del gestore al fine di non perdere i dati. Si evidenzia pertanto tale potenziale criticità e la conseguente necessità che siano attuate adeguate misure, anche organizzative, rivolte a minimizzare detto rischio.

I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs. 30 giugno 2003, n. 196.

Tenuto conto di quanto sopra indicato, il mantenimento del parere positivo nel tempo soggiace pertanto alla persistente implementazione di adeguate misure tecniche ed organizzative da parte del responsabile esterno gestore della piattaforma, che il Titolare dovrà monitorare costantemente. Altresì determinanti risultano le modalità del trattamento da parte dei soggetti interni allo stesso preposti, per cui le istruzioni agli stessi impartite e la loro adeguata formazione costituiscono un aspetto da presidiare continuativamente da parte dello stesso Titolare.

Data della firma digitale

Il Responsabile Protezione Dati
Riccardo Narducci

Riccardo Narducci | Firmato digitalmente da: Riccardo Narducci
Data: 23/04/2026 16:29:18