COMUNE DI CASALETTO CEREDANO IT00330940198
Via Guglielmo Marconi, 10 Casaletto Ceredano - 26010, Casaletto Ceredano (CR) - Italia
0373 262305 Info@comune.casalettoceredano.cr.it

Report delle valutazioni d’impatto per COMUNE DI CASALETTO CEREDANO

Informazioni generali

Esportate **1 valutazioni d’impatto**.

Legale rappresentante

Nome e cognome	Email	Telefono fisso	Cellulare	PEC
Aldo Casorati	sindaco@comune.casalettoceredano.cr.it	0373 262305	-	-

Valutazioni d’impatto esportate (1 totale/i)

Adempimenti relativi al Whistleblowing

	Stato valutazione	Attiva
TRATTAMENTI	Adempimenti relativi al Whistleblowing	
IDENTIFICAZIONE	**Natura, ambito di applicazione, contesto e finalità del trattamento considerate**	**Sì**, Le informazioni sulle violazioni di cui i segnalanti sono venuti a conoscenza nell’ambito del contesto lavorativo vanno trasmesse al Responsabile della Prevenzione della Corruzione e Trasparenza (RPCT) esclusivamente attraverso il canale interno. Nel caso in cui la segnalazione pervenga ad un soggetto diverso da quello previsto (ad esempio un Responsabile di Settore) tale soggetto deve trasmettere la segnalazione, entro sette giorni dal suo ricevimento, al RPCT del Comune di Casaletto Ceredano, adottando le misure necessarie a garantire la riservatezza e dando contestuale notizia della trasmissione alla persona segnalante
	Dati pers., destinatari e il periodo di conserv. registrati	**Sì**, È necessario che la segnalazione sia il più possibile circostanziata al fine di consentire la delibazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni negli enti e amministrazioni del settore pubblico e privato nonché da parte di ANAC. In particolare è necessario risultino chiare: • le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione; • la descrizione del fatto; • le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati. È utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l’indicazione di altri soggetti potenzialmente a conoscenza dei fatti Conservati 5 anni
	Descrizione funzionale del trattamento fornita	**Sì**, Il canale interno attivato dal Comune di Casaletto Ceredano per la ricezione della segnalazione di violazioni prevede l’utilizzo di una procedura informatica. L’accesso alla procedura informatica avviene tramite il link pubblicato nel portale del Comune di Casaletto Ceredano, alla pagina dedicata. La gestione del canale interno di segnalazione è affidata al RPCT del Comune di Casaletto Ceredano, che si avvale di un fornitore esterno di servizi informatici per l’implementazione della procedura informatica, il quale è stato nominato Responsabile del trattamento ai sensi dell’art. 28 GDPR nonché amministratore di sistema. La procedura informatica di segnalazione interna garantisce, attraverso l’applicazione di strumenti di crittografia, la riservatezza dell’identità del segnalante, del facilitatore, delle persone coinvolte o comunque menzionate nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione in tutte le fasi della procedura medesima. Tali informazioni saranno accessibili esclusivamente al RPCT ed alle persone specificamente incaricate per la gestione delle segnalazioni. Il sistema informatico rilascia al segnalante una ricevuta contenente il Key code, la cui conservazione è necessaria al fine di accedere ed eventualmente modificare la segnalazione precedentemente effettuata presso il portale. Il RPCT è l’unico soggetto abilitato, mediante specifiche credenziali di accesso al portale, alla lettura delle segnalazioni e, pertanto, è responsabile della custodia di tali credenziali ed adotta ogni precauzione perché nessun altro possa acquisirle o accedere al portale per mezzo delle stesse.
	Risorse dei dati pers. individuate	**Sì**, Whistelblowingit:il Comune, in ossequio alle prescrizioni di cui al decreto legislativo 10 marzo 2023, n. 24, che recepisce in Italia la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, intende aderire al progetto Whistleblowing PA, nato dalla volontà di Transparency International Italia di offrire a tutte le Pubbliche Amministrazioni un software informatico gratuito (disponibile al link whistleblowing.it) per dialogare con i segnalanti, grazie a modalità che garantiscono eventualmente l’anonimato; con decreto sindacale n. 29 del 10.01.2023 con cui il Segretario Comunale, Dott. Francesco Rodolico, è stato nominato Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT);
	Tenuto conto del rispetto dei codici di condotta approvati	**No**, -
NECESSITÀ	**Finalità determinate**	**Sì**, il PNA impone alle pubbliche amministrazioni, di cui all’art. 1, comma 2, del D.Lgs 165/2001, l’assunzione dei “necessari accorgimenti tecnici per dare attuazione alla tutela del dipendente che effettua le segnalazioni”.
	Finalità esplicite	**Sì**, il Piano Nazionale Anticorruzione (PNA), approvato con la deliberazione n. 72 dell’11settembre 2013 dall'Autorità Nazionale Anticorruzione, riconduce espressamente la tutela del dipendente che segnala condotte illecite, tra le azioni e misure generali finalizzate alla prevenzione della corruzione, in particolare fra quelle obbligatorie;
	Finalità legittime	**Sì**, l’art. 4 del D.lgs. 24/2023, a mente del quale: “I soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano, ai sensi del presente articolo, propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. I modelli di organizzazione e di gestione, di cui all'articolo 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto. 2. La gestione del canale di segnalazione e'

		affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero e' affidata a un soggetto esterno, anch'esso autonomo e con personale specificamente formato. 3. Le segnalazioni sono effettuate in forma scritta, anche con modalità informatiche, oppure in forma orale. Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole. 4. I comuni diversi dai capoluoghi di provincia possono condividere il canale di segnalazione interna e la relativa gestione. I soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a duecentoquarantanove, possono condividere il canale di segnalazione interna e la relativa gestione. 5. I soggetti del settore pubblico cui sia fatto obbligo di prevedere la figura del responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, affidano a quest'ultimo, anche nelle ipotesi di condivisione di cui al comma 4, la gestione del canale di segnalazione interna. 6. La segnalazione interna presentata ad un soggetto diverso da quello indicato nei commi 2, 4 e 5 e' trasmessa, entro sette giorni dal suo ricevimento, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante.”
	Trattamenti leciti	**Sì**, il Piano Nazionale Anticorruzione (PNA), approvato con la deliberazione n. 72 dell’11settembre 2013 dall'Autorità Nazionale Anticorruzione, riconduce espressamente la tutela del dipendente che segnala condotte illecite, tra le azioni e misure generali finalizzate alla prevenzione della corruzione, in particolare fra quelle obbligatorie **Motivi:** Obbligo di legge
	Dati pers. adeguati	**Sì**, Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l’erogazione dei servizi in modalità SaaS così come pattuito tra le parti. Dati di registrazione Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione). Categorie particolari di dati Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati. Dati relativi a condanne penali e reati Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.
	Dati pers. limitati	**Sì**, Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell’utente che effettua la registrazione e i dati relativi all’ente (nome, indirizzo, CF e PI).
	Definiti limiti di conserv.	**Sì**, Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte.
DIRITTI	**Interessati informati**	**Sì**, L'informativa è implementata e consultabile.
	Accesso garantito	**Sì**, L'interessato può accedere ai propri dati personali tramite piattaforma.
	Portabilità garantita	**Sì**, L'interessato può richiedere il trasferimento dei propri dati su supporto elettronico.
	Rettifica garantita	**Sì**, L'interessato può rettificare i dati errati contenuti nella propria registrazione e/o nella segnalazione.
	Cancellazione garantita	**Sì**, Il diritto di cancellazione è garantito, fatti salvi i termini di legge.
	Opposizione garantita	**Sì**, L'interessato può effettuare opposizione al RPCT.
	Limitazione garantita	**Sì**, I dati personali utilizzati sono strettamente limitati a quelli necessari; in caso di dati eccedenti l'interessato può fare segnalazione al RPCT e/o al DPO.
	Gestiti rapporti con resp.	**Sì**, I responsabili e subresponsabili esterni sono individuati, istruiti e nominati.
	Consultazione preventiva	**No**, Non necessaria.
RISCHI	**Accesso non autorizzato ai dati utente**	**DATI GENERALI**
		Fonti di rischio: Terza parte malintenzionata, Incidente o disastro
		Impatti potenziali: Sentimento di violazione della privacy e danno irreparabile
		Minacce: Attacco informatico
		VALUTAZIONE DEL RISCHIO
		Probabilità (P): 1
		Gravità (G): 3
		Rischio (P x G): **Basso** (3/16)

Rischio ridotto	**Basso** (3/16)
MISURE	
Misura	Crittografia
Attuazione	L’applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l’Open Technology Fund di Washington. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto. Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html
Addetti attuazione	
Da attuare entro	-
Attuata	Sì
Data attuazione	01/10/2023
Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
Misura	Controllo degli accessi
Attuazione	L’accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.
Addetti attuazione	
Da attuare entro	-
Attuata	Sì
Data attuazione	01/10/2023
Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
Misura	Tracciabilità
Attuazione	L’applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.
Addetti attuazione	
Da attuare entro	-
Attuata	Sì
Data attuazione	01/10/2023

Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
Misura	Archiviazione
Attuazione	L’applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell’applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura
Addetti attuazione	
Da attuare entro	-
Attuata	Sì
Data attuazione	01/10/2023
Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
Misura	Backup
Attuazione	I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.
Addetti attuazione	
Da attuare entro	-
Attuata	Sì
Data attuazione	01/10/2023
Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
Misura	Sicurezza dei siti web
Attuazione	Tutte le connessioni sono protette tramite protocollo TLS 1.2+ Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.
Addetti attuazione	
Da attuare entro	-
Attuata	Sì
Data attuazione	01/10/2023
Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
Misura	Manutenzione
Attuazione	E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l’infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.
Addetti attuazione	

		Da attuare entro	-
		Attuata	Sì
		Data attuazione	01/10/2023
		Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
		Misura	Sicurezza dell'hardware
		Attuazione	I datacenter del fornitore IaaS dispongono di un’infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. I datacenter del fornitore IaaS sono certificati ISO27001
		Addetti attuazione	
		Da attuare entro	-
		Attuata	Sì
		Data attuazione	01/10/2023
		Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
		Misura	Lotta contro il malware
		Attuazione	Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell’arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.
		Addetti attuazione	
		Da attuare entro	-
		Attuata	Sì
		Data attuazione	01/10/2023
		Riduzione rischio	Molto (Agisce sulla probabilità del rischio)
INTERESSATI	**DPO consultato**	**Sì**, Consultato e aggiornato su procedure e scelta del software	
	Opinioni degli interessati raccolte	No, Non necessarie in quanto obbligo di legge	
CONCLUSIONI	**Parere del DPO**	Il DPO esprime parere favorevole quanto le misure tecniche e organizzative adottate risultano adeguate.	
	Conclusioni finali	Si ritiene che il trattamento garantisca la sicurezza dei dati degli interessati come prescritto dalla normativa.	
REVISIONI	**Periodicità**	1 anno	
	Ultima revisione	16/12/2023	
	Prossima revisione	31/12/2024	

COMUNE DI CASALETTO CEREDANO IT00330940198
Via Guglielmo Marconi, 10 Casaletto Ceredano - 26010, Casaletto Ceredano (CR) - Italia
0373 262305 Info@comune.casalettoceredano.cr.it