- Whistleblowing – Attivo

Processo di trattamento	Whistleblowing
Descrizione del processo	Gestione delle segnalazioni di condotte illecite ricevute mediante apposita piattaforma informatica. Tale attività, in sintesi, consiste nel: prendere in carico la segnalazione; verificare la rilevanza della segnalazione ai sensi di quanto previsto dalla disciplina in materia di whistleblowing; classificare la segnalazione; raccogliere documentazione, informazioni o altro materiale necessario per valutare la segnalazione; eventuale interlocuzione con il soggetto segnalante e/o con altri soggetti coinvolti; dare riscontro al segnalante; chiudere la segnalazione.
Natura del dato trattato e policy di cancellazione del dato	- Dati personali comuni del segnalante (nome, cognome); - Dati personali comuni del segnalato; - Altri dati comuni e/o particolari e/o riferiti a condanne penali e reati riportati nella segnalazione o raccolti durante l'attività di gestione della stessa - Dati comuni e/o particolari e/o riferiti a condanne penali e reati di altri soggetti coinvolti Tutti i dati personali saranno conservati 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.
Finalità del trattamento	Gestione delle segnalazioni
Base giuridica	- Obbligo di legge (dati comuni e riferiti a condanne penali e reati) - Motivi di interesse pubblico rilevante ai sensi dell'art. 9, c.2 lettera g) del REG. UE 679/2016 (dati particolari)
Ruoli	Titolare del trattamento: Garda 2015 s.c.s. Interessato: Soggetto segnalante Interessato: Soggetto segnalato Interessato: Altro soggetto coinvolto nella segnalazione Responsabili esterni: Federazione Trentina della Cooperazione [gestore delle segnalazioni] Sub-Responsabile: [fornitore piattaforma] Whistleblowing Solutions
Trasferimento extra EU	No
Tecnologie del trattamento	Archivio cartaceo Piattaforma WhistleblowingPA
Misure di sicurezza	<u>Misure della piattaforma e del fornitore della piattaforma:</u> - Firewall perimetrale - Segregazione della rete in molteplici VLAN - Crittografia - Policy sicurezza password e autenticazione a due fattori - Accessi separati per utenti diversi - Connessioni amministrative privilegiate mediate tramite accesso VPN Sistema di registrazione log accessi degli amministratori - Audit di sicurezza periodici e non periodici - Sistema di backup remoto giornaliero - Manutenzione periodica - Sicurezza fisica dei locali del datacenter - Procedura per la gestione di data breach adottata dal sub-responsabile <u>Misure del soggetto gestore:</u>

	- Computer utilizzati dal Responsabile per accedere alla piattaforma dotati di antivirus, firewall, sistema di gestione password (complessità e scadenza), sospensione pc - Procedura per la gestione di data breach - Regolamento per la protezione dei dati (contenente istruzioni agli autorizzati per un corretto trattamento dei dati personali, utilizzo dei dispositivi informatici e di Internet) - Autorizzazione al trattamento dati con apposite istruzioni operative - Formazione in tema di protezione dei dati personali