
COMPLIANT CON IL
CODICE DI CONDOTTA SOFTWARE

Oggetto: Comunicazione di esito della valutazione della domanda di adesione al Codice di Condotta

Zucchetti S.p.A. – MyGo S.r.l.

Data: 9 febbraio 2026

Prot. ODM: Z03-2025

Destinatario:

MyGo S.R.L.
Alla cortese attenzione del Responsabile

1. Premessa

Facciamo seguito alla Vostra domanda di adesione al Codice di Condotta dei Produttori di Software, presentata per il prodotto My Whistleblowing di MyGo S.R.L. L'Organismo di Monitoraggio (ODM) ha completato la valutazione della documentazione pervenuta, riscontrando un livello di maturità complessivo elevato e pienamente coerente con i principi del Codice.

In esito a tale valutazione, l'adesione di MyGo S.R.L. per il prodotto My Whistleblowing al Codice di Condotta dei Produttori di Software viene formalmente accolta. Nel corso dell'analisi sono stati individuati alcuni aspetti documentali e tecnici che potranno essere ulteriormente approfonditi e completati nel quadro delle attività di monitoraggio periodico previste dall'ODM.

2. Aree di integrazione e miglioramento

L'ODM riconosce la solidità complessiva della documentazione trasmessa e la coerenza del prodotto My Whistleblowing con i principi del Codice di Condotta. In un'ottica di perfezionamento continuo, si richiedono tuttavia alcune integrazioni e aggiornamenti documentali su aree ritenute rilevanti per il mantenimento della conformità e la trasparenza verso gli utenti finali.

N.	Area di riferimento	Descrizione sintetica	Livello di priorità	Indicazioni ODM
1	Gestione operativa	Fornire evidenze aggiornate sulle attività di test e manutenzione correttiva per dimostrare la continuità del monitoraggio tecnico.	Media	Condividere con l'ODM i principali piani di controllo periodico o report interni disponibili.
3	Backup e riservatezza	Integrare informazioni relative alle procedure di backup e protezione nei processi di condivisione o trasferimento dati.	Media	Fornire evidenze sintetiche o riferimenti documentali già disponibili.

Si nota preliminarmente quanto segue per il Requisito di dettaglio (RD) RD01.1, per la soddisfazione del quale nessuna ulteriore evidenza qui si richiede, basandosi sulla corrente iniziale versione del modello di Auto-dichiarazione. Pertanto, questo punto costituisce un semplice riflessione, di cui l'azienda produttrice potrà decidere se utilizzare o meno in futuro.

RD01.1 Analisi di nuove funzioni. Il documento SDLC Policy riferito e allegato all'auto-dichiarazione tratta di un Software Development Life Cycle, SDLC, e non di un SSDLC - Security SDLC - e tanto meno DPSSDLC - Data Privacy & SSDLC. Nei fatti il documento riferito mai nomina Data Privacy e utilizza - in modo del tutto generico - un paio di volte il termine Security e una sola volta termini con radice "Minimiz", di cui al requisito di dettaglio. Si dichiara altresì che viene impiegato un approccio Agile, ma non si capisce il

tipo di tale approccio e quale ruolo, dove e quando definisce i Test di Accettazione per la prossima iterazione. Anche varie altre cose scritte nel documento non risultano del tutto chiare.

Si chiede altresì di comunicare versione e release, se esistenti, del prodotto sottoposto a questo ODM per adesione al Codice di condotta.

Si evidenziamo (E) qui di seguito alcune rilevazioni per gli indicati Requisiti di dettaglio.

E1. RD02.2 Documentazione degli strumenti e dei requisiti per l'utilizzo del SW. Il produttore dichiara di utilizzare AWS. Successivamente, in corrispondenza di un altro Requisito di dettaglio (R.29), è scritto che i dati sono allocati presso centri Amazon in Francoforte e Irlanda. *Si può intendere che ivi sono anche allocate repliche e backup, nonché in nessun caso è autorizzato il trasferimento di dati in Europa orientale o altri continenti?* Se no, indicare gli altri stati possibilmente destinatari dei dati.
E2. RD03.1 Modalità e regole di autenticazione. Nei documenti riferiti (SLC e My Governance _ Secure platform & Architecture), è scritto "L'archiviazione cloud che non sia quella tramite il proprio software [Ndr: aziendale] My Archives è consentita da MYGO solo se -tale azione è in accordo con la classificazione di sicurezza delle informazioni; -… *Si potrebbe chiarire o esemplificare tale affermazione?*
E3. RD03.4 Autenticazione/API. Bisognerebbe descrivere o riferire la politica adottata in materia da AWS.
E4. RD08.1 Sicurezza Sw/Secure coding. Nel paragrafo Frequenza scansione di vulnerabilità del documento Policy sulla gestione delle vulnerabilità, andrebbe completata l'espressione: "Le tempistiche di cui sopra potranno essere comunque specificate dal management anche alla".
E5. RD08.2 Sicurezza Sw/Minacce e vulnerabilità. Idem RD08.1.
E6. RD09.1 Log applicativi di attività utente. Sebbene il citato "log più puntuale è attivabile opzionalmente" andrebbe dettagliato, la dichiarazione si può ritenere sufficiente.
E7. RD11.1Data retention. "Screen tool per gestione data retention segnalazioni in allegato". **MANCA**. Allegato non trovato. Nell'auto-dichiarazione, bisognerebbe riferire i file allegati con il loro nome!
E8. RD12.1 Formazione, nel file di nome Corsi2026 è riportato una Programmazione Corsi Formativi 2026. Nulla è detto in merito al presente e al passato.
E9. RD13.1 Librerie. "screen shot gruppi librerie". È necessario che sia qui scritto il nome del file riferito. Solo pochi degli screen shot allegati. sono auto-documentanti.

E10. RD14.1 Autorizzazione e autenticazione. Il requisito pone, peraltro, la seguente domanda, la quale attende tuttora risposta: *le utenze degli operatori di assistenza sono o non sono periodicamente revisionate allo scopo di verificare che i permessi e le autorizzazioni di accesso siano sempre aggiornate?* Descrivere come ciò accade o inserire riferimenti a documenti.

E11. RD14.2 Assegnazione dei privilegi. Il requisito pone, peraltro, la seguente domanda, la quale ancora attende risposta: *gli operatori autorizzati a erogare assistenza possono navigare come vogliono sui dati del cliente o ci sono dei limiti imposti e se sì quali?* Descrivere tali eventuali limiti o inserire riferimenti a documenti.

E12. RD14.3 Password policy. *Numero minimo e tipo di caratteri, periodo temporale di sostituzione per le varie tipologie di utenze?*

E13. RD14.4 Utilizzo della VPN. L'operatore di assistenza: l) *accede da remoto alla piattaforma del cliente mediante connessione VPN con MFA oppure no?* 2) *Prima dell'utilizzo di ogni sessione, c'è o no l'autorizzazione del Cliente ed è poi quest'ultimo ad attivare o disattivare l'accesso ai propri sistemi in relazione alle richieste e alle attività svolte?* 3) *Al termine dell'intervento l'operatore di assistenza comunica al cliente la fine dell'intervento e richiede la disattivazione dell'accesso?* Descrivere come ciò accade o inserire riferimenti a documenti.

E14. RD15.1 Patch management. Ci si aspetta di leggere numeri su tempistiche e aggiornamenti del patching dell'erogazione assistenza.

E15. RD17.2 Gestione sistema di supporto. *Bisogna intendere che nessuna autorizzazione è richiesta al cliente in modo tracciabile? E' il cliente che può andare al ticket e osservare l'evoluzione dello stato?*

E16. RD18.01 Consulto interna all'ODM riferisce su ammissibilità di quanto menzionato dall'azienda on documento allegato all'Auto-dichiarazione in relazione al rispetto del requisito.

E17. RD20.1 Utilizzo dei dati per esecuzione dei test. Salvo diversa comunicazione del produttore, intendiamo che per i test sono sempre usati solo dati fittizi. Vorremmo però leggere le indicazioni a riguardo esplicitamente date agli operatori di assistenza per il test. *Quale è ilnome del relativo documento?* Allegare tale file.

E18. R22.3e Attività di migrazione e conversione. "Specifico PLA dato al cliente per la parte di Conversione da concorrenza. *PLA: è da intendersi Programmable Logic Array o che altro? Che cosa si deve intendere qui per concorrenza?* -

Le valutazioni espresse si basano sulla documentazione e sulle evidenze tecniche condivise in fase di istruttoria. L'Organismo di Monitoraggio resta comunque pienamente disponibile a un confronto con i referenti aziendali, qualora si ritenesse utile approfondire specifici

aspetti delle aree indicate o concordare modalità operative per l'invio di eventuali integrazioni o aggiornamenti.

3. Criteri di audit e gestione della verifica

L'ODM effettuerà le attività di audit e verifica a campione sulle aziende aderenti al Codice di Condotta, in coerenza con le proprie procedure di controllo. Le organizzazioni con documentazione completa saranno considerate a minor priorità di audit, mentre quelle con integrazioni in sospeso potranno essere selezionate con maggiore probabilità per verifiche approfondite.

4. Chiusura

L'Organismo di Monitoraggio riconosce l'impegno di MyGo S.R.L. nel percorso di adesione e valuta positivamente il livello di conformità raggiunto dal prodotto HR Portal. Le integrazioni e gli aggiornamenti proposti rappresentano un passaggio naturale nel percorso di miglioramento continuo previsto dal Codice di Condotta.

Cordiali saluti,
Fondazione ODM Software ETS
Organismo di Monitoraggio accreditato ai sensi dell'art. 41 GDPR