Rilasciata nel novembre 2025

Dichiarazione di conformità del software alle normative vigenti

Nome del software: Sportello Telematico Polifunzionale

Nome del produttore: Maggioli S.p.A. (nel seguito "**Maggioli**" o la "**Società**")

Dati del produttore: sede legale in Via Del Carpino n.8 (47822) Santarcangelo di Romagna (RN) - Italia, P.IVA. 02066400405

La scrivente Società in qualità di software house che ha sviluppato il sistema informativo cloud nativo "Sportello Telematico Polifunzionale", dichiara che nella versione rilasciata -come da note di rilascio pubblicate sul sito web dedicato alle release software- è conforme alle seguenti norme e standard:

- *"Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale"* (Agenzia per la Cybersicurezza Nazionale) D.P.C.M. 9 dicembre 2021, n. 223;
- Direttiva (UE) 2022/2555 (NIS2), recepita in Italia con il Decreto Legislativo 4 settembre 2024, n. 138;
- Regolamento Generale sulla protezione dei dati (Reg. EU. 2016/679);
- Software Assurance Maturity Model (SAMM) come metodologia di DevSecOps e standard metodologico per l'integrazione della sicurezza informatica sin dalla fase di sviluppo;
- Domain Driven Design come standard metodologico di progettazione;
- Certificazioni che attestano la creazione, l'applicazione ed il mantenimento dei Sistemi Gestionali ed Organizzativi di Maggioli S.p.A. conformi alle norme, consultabili al seguente link: https://www.maggioli.com/it-it/chi-siamo/certificazioni

Descrizione del software, comprese le sue funzionalità e scopi

Sportello Telematico è un'applicazione web che consente ai cittadini di interagire con la Pubblica Amministrazione in modo digitale, senza la necessità di recarsi fisicamente presso gli uffici. Attraverso questa piattaforma, è possibile accedere a una vasta gamma di servizi online, come la presentazione di istanze, la consultazione di documenti, il pagamento di tributi e la richiesta di certificati. L'utente deve accedere alla piattaforma tramite le proprie credenziali, come SPID, CIE o CNS, garantendo così la sicurezza e l'autenticità dell'interazione. Successivamente, può navigare tra le diverse sezioni del portale e individuare il servizio d'interesse. A questo punto, l'utente viene guidato nella compilazione di moduli online, nell'upload di documenti necessari e, se previsto, nel pagamento di eventuali oneri tramite sistemi di pagamento elettronico integrati. Una volta completata la procedura, l'utente riceve una ricevuta digitale che attesta l'avvenuta presentazione della richiesta. Lo Sportello Telematico offre inoltre la possibilità di monitorare lo stato di avanzamento delle pratiche presentate e di ricevere notifiche in tempo reale sugli aggiornamenti.

Il software è stato sviluppato e testato in conformità con le seguenti procedure:

- Per ottimizzare il ciclo di vita del software, è stata adottata la metodologia SAMM (Software Assurance Maturity Model) di OWASP (consultabile al link https://owasp.org/www-project-samm/) come standard per i gruppi di sviluppo. Questa metodologia, caratterizzata da semplicità, flessibilità e compatibilità con i processi esistenti, guida il miglioramento continuo delle pratiche di sicurezza del software in relazione all'intercettazione delle vulnerabilità in ogni fase di progettazione del prodotto.
- Applicata a tutti i prodotti con un ciclo di vita a lungo termine, SAMM prevede una valutazione iniziale (assessment) per determinare lo stato attuale della sicurezza e definire una roadmap di miglioramento. Il modello suddivide il ciclo di vita del software in cinque funzioni aziendali: Governance, Design, Implementation, Verification e Operation. A ciascuna pratica, infatti, viene assegnato un punteggio da 0 a 3, il quale indica il livello di maturità della sicurezza. La roadmap di

miglioramento, definita dal team di sviluppo in collaborazione con il Responsabile Sicurezza, stabilisce obiettivi e tempi specifici per elevare il livello di sicurezza del software, e il più grande pregio di tale metodo è quello di avere una fotografia dello stato di sicurezza del software sempre aggiornata, così da poter individuare i rischi e apportare, di volta in volta, le misure di correzione e mitigazione più appropriate.

- L'intero processo di discovery delle vulnerabilità è sottoposto a un continuo aggiornamento e monitoraggio. Per questo, si utilizza un software di bug tracking evoluto, integrato con un sistema di help desk, il cui obiettivo è quello di rendicontare il ciclo di vita delle issue create dall'assistenza. Tale software è integrato anche con un servizio SaaS per la gestione del codice, il quale viene utilizzato per la referenziazione del codice relativo alle issue. Le risoluzioni di ogni issue sono pubblicate sotto forma di "note" all'interno di un portale dedicato alle release, garantendo un monitoraggio costante e completo di ogni azione intrapresa per la risoluzione delle vulnerabilità.

Sintesi delle misure tecniche e organizzative generali

- **Gestione Utenti e accessi**

Il sistema di autenticazione degli utenti alle applicazioni in oggetto permette di integrarsi in modo efficace con i sistemi pubblici di identità, in particolare SPID e CIE, oltre al proprio sistema interno di autenticazione può integrarsi ai sistemi dei clienti mediante tecnologie di Single Sign On basate su protocolli standard (es. OAuth2, OpenID, SAML). L'autenticazione degli utenti è prevista una sola volta, al momento dell'accesso all'applicazione. L'applicazione prevede funzionalità di tipo amministrativo, tali da consentire una profilazione centralizzata e granulare degli utenti.

- **Protezione dati personali**

Le attività svolte sui dati personali sono strettamente necessarie e non eccedenti a quanto richiesto dal Titolare del trattamento, che ne mantiene la proprietà esclusiva. L'azienda adotta misure tecniche e organizzative per garantire la sicurezza del trattamento dei dati, che includono la protezione delle aree fisiche e dei locali, la corretta archiviazione di documenti e supporti, e la sicurezza logica degli strumenti elettronici e del portale. Per il trattamento dei dati tramite strumenti elettronici, sono implementati un sistema di autenticazione informatica e policy di autorizzazione che definiscono i tipi di dati accessibili in base alle mansioni lavorative. Il sistema è inoltre protetto da malfunzionamenti e

attacchi informatici tramite firewall e antivirus centralizzati

- **Requisiti minimi di sicurezza**

I requisiti minimi di sicurezza previsti dalle Linee Guida per la sicurezza informatica prevedono una serie di misure atte a garantire la protezione dei sistemi informativi e dei dati gestiti dalle Pubbliche Amministrazioni.
Si sottolinea come il tema non riguardi esclusivamente la privacy del dato, ma anche la sua integrità e disponibilità. Per mitigare il rischio di incorrere in problematiche di questo tipo è introdotta una sezione dedicata alla valutazione RID sin dalla fase di analisi delle funzionalità (correttive, adeguative ed evolutive) prima di introdurle all'interno della catena produttiva. Questo permette di esaminare preventivamente gli impatti di una modifica software su dati potenzialmente sensibili e di focalizzare le fasi di collaudo sui punti più critici.

- **Gestione dei Log**

Il software è dotato di un sistema di audit e logging per le operazioni delle macro-entità, che registra le attività di creazione, lettura, aggiornamento ed eliminazione (CRUD) su apposite tabelle di sistema. Per le modifiche, in particolare, vengono acquisite le informazioni sia prima che dopo l'aggiornamento. I log contengono riferimenti temporali e una descrizione dettagliata dell'evento tracciato, garantendo la completezza e l'inalterabilità dei dati registrati. Le entità da tracciare sono configurabili, permettendo di abilitare o disabilitare il logging per specifiche entità o per interi microservizi. Tutti i log sono accessibili tramite una specifica funzione, disponibile esclusivamente per i profili abilitati, per semplificare le attività di monitoraggio e verifica.

- **Cifratura**

Le metodologie crittografiche adottate sono pienamente conformi alle linee guida e ai requisiti stabiliti dall'Agenzia per la Cybersicurezza Nazionale (ACN).
La strategia implementata si basa sull'adozione della Transparent Data Encryption (TDE), una tecnica di crittografia dei dati a riposo che opera a livello di database. L'obiettivo principale di questa misura è la protezione dei dati sensibili e personali "at rest" mediante la cifratura dell'intero database, inclusi i file di dati, di registro e di backup.
Questa tecnologia è implementata e sfruttata in modo nativo o tramite personalizzazioni in base al Cloud Provider scelto per l'erogazione dei servizi.

Nel contesto della piattaforma PaaS Maggioli, che si avvale dell'architettura Google Cloud, la TDE opera sul database Cloud SQL MySQL, gestendo automaticamente le chiavi di crittografia (DEK e KEK) attraverso il Key Management Service (KMS) di Google. Ciò garantisce elevati livelli di sicurezza grazie alla gestione centralizzata delle chiavi e a meccanismi di backup sicuri, con crittografia automatica sia dei dati a riposo che in transito.

Gestione degli incidenti di sicurezza – Violazione dei dati (art. 33 e 34 del GDPR)

Maggioli S.p.A. ha adottato una procedura di Incident Response per gestire eventi di sicurezza informatica e Data Breach, in linea con il GDPR e le norme ISO, per migliorare la propria sicurezza. Un Data Breach è definito come la perdita di riservatezza, integrità o disponibilità (RID) dei dati personali.
Eventi comuni che possono causare un Data Breach includono furto/smarrimento di dispositivi contenenti dati personali, perdita/modifica di archivi, diffusione impropria di dati (es. email errate), attacchi informatici, divulgazione a persone non autorizzate e violazioni della sicurezza fisica.
Per gestire questi eventi, Maggioli ha istituito un "Team di Crisi", responsabile del rilevamento, contenimento e risoluzione degli incidenti. Il team include DPO, CISO, Ufficio Privacy, Ufficio Legale, Consulente Privacy e Team Security. Ogni area aziendale ha un referente che collabora con il Team di Crisi.

Il processo di gestione degli incidenti si articola in quattro fasi:

1. Scoperta: Segnalazione dell'incidente e compilazione del registro.
2. Qualificazione: Il Team di Crisi valuta l'evento.
3. Valutazione: CISO, Team di Crisi e DPO decidono la risposta proattiva.
4. Azione: Implementazione di misure correttive a breve e lungo termine.

L'Ufficio Privacy è il punto di contatto iniziale per tutte le segnalazioni. Il CISO e il DPO, in collaborazione con l'Ufficio Privacy, qualificano l'evento come Data Breach o semplice evento di sicurezza. Il registro dell'incident report deve essere finalizzato entro 8 ore dalla presa in carico dell'evento e trasmesso al Team di Crisi, il quale valuta anche l'evento e il

rischio per gli interessati, decidendo se è necessaria una notifica al Garante o al cliente.

Le tempistiche di notifica variano, sempre in ottemperanza con quanto previsto agli art. 33 e 34: se Maggioli è Titolare del trattamento, la notifica all'Autorità Garante deve avvenire entro 72 ore, salvo improbabile pregiudizio per i diritti degli interessati, mentre invece se Maggioli è Responsabile del trattamento, le tempistiche sono stabilite dal Titolare, generalmente 24-48 ore per la trasmissione di una relazione tecnica

Sintesi delle misure tecniche ed organizzative per la protezione dei dati personali relative ad installazioni con Container orchestrator

- Configurazione Sicura: sono state implementate procedure secondo i principi di sicurezza by design e hardening della configurazione dell'orchestratore
- Autenticazione e Autorizzazione: sono stati implementati metodi di autenticazione e autorizzazione applicando il principio del minimo privilegio su utenti, service account e workload.
- Sicurezza dei Container: Vengono utilizzate e mantenute aggiornate immagini ufficiali, firmate, minimizzate. Le immagini vengono sottoposte a scansione per rilevare vulnerabilità.
- Crittografia delle Comunicazioni: Uso di protocolli sicuri per le connessioni esterne
- Cifratura e Protezione dei Dati: E' abilitato l' encryption at rest per volumi e secrets
- Logging e Monitoring: Log degli eventi e audit log attivi con alerting su eventi critici e anomali
- Aggiornamenti e Patch: Sono stati implementati automatismi e procedure per mantenere tutti i componenti aggiornati con le ultime patch di sicurezza.
- Controllo delle Risorse: Sono stati previsti e applicati limiti alle risorse in modo da poter prevenire attacchi DDoS.
- Sicurezza dello Storage: L'accesso ai volumi persistenti è stato opportunamente hardenizzato e configurato in sicurezza.
- Controllo della Supply Chain: Sono state verificare e gestire le dipendenze di terze parti in modo da limitare attacchi e minacce.
- Backup e Disaster Recovery Sicuri: Backup policy versionata con test di restore automatizzati
- Formazione e Consapevolezza: formazione del personale su best practice e minacce

Audit e monitoraggio del software

L'azienda esegue periodicamente test di Vulnerability Assessment (VA) e Penetration Testing (PT) sui sistemi ritenuti più critici o che hanno avuto maggiori segnalazioni. Tali test sono affidati a un'azienda terza e vengono condotti, indicativamente, in due sessioni annuali, a distanza di sei mesi l'una dall'altra, per consentire la correzione delle eventuali vulnerabilità riscontrate nella prima fase. Per evitare ripercussioni operative, i test vengono eseguiti esclusivamente su ambienti di test dedicati. Le remediation e le best practice identificate sono applicate e verificate su questi ambienti prima del rilascio in produzione, assicurando l'assenza di regressioni. Oltre ai test annuali eseguiti da un fornitore esterno, l'azienda si avvale di un software di scansione automatico per l'esecuzione continua di VA e PT su tutti gli ambienti di test dei propri prodotti.

Servizio di assistenza clienti

L'assistenza viene garantita mediante un servizio di help-desk, per fornire il supporto tecnico-operativo agli utenti dell'Ente interessati alla fruizione dei servizi dell'infrastruttura tecnologica ed applicativa. Il servizio di help-desk eroga le sue attività agli utenti al fine di risolvere le problematiche che si manifestano e per le quali il personale dell'Ente non sia autonomo nella soluzione. Il servizio di help desk viene erogato da personale altamente qualificato, preparato e di comprovata esperienza nel settore della Pubblica Amministrazione Locale ed è in grado di risolvere in modo rapido e puntuale il problema segnalato.

Compiti ed attività del servizio di Help desk sono tali da:

- fornire direttamente la soluzione attraverso il canale telefonico e/o con collegamento da remoto, avvalendosi in caso di necessità del supporto del 2° Livello e/o del reparto di Sviluppo software.
- attivare su richiesta del Cliente, previo acquisto di giornate, l'assistenza on site di personale in modalità affiancamento nel caso di esigenza specifica dell'ente.