Autore	Ufficio privacy
Approvazione	Alberto Cazzulani

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio privacy	01/11/2026	01/11/2026	Prima emissione

PARERE DPO OK

MY-WB 2.0

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Zucchetti Spa				
Partita Iva	05006900962				
Indirizzo	Piazza Mino Zucchetti,1				
Città	Lodi	**Cap**	26900	**PV**	LO
Legale Rappresentante	Alessandro Zucchetti preposto dalla società CONVERTENDO SRL, Legale rappresentante di Zucchetti SPA				

STRUTTURA ORGANIZZATIVA			
Divisione	Divisione HR	Responsabile Divisione	Uggeri Domenico
Area	Area Piattaforma Base HR & Tools	Responsabile Reparto	Alberto Cazzulani

INCARICATI DEL TRATTAMENTO
Addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti

DATI DI CONTATTO			
Responsabile del trattamento	Zucchetti Spa	ufficio.privacy@zucchetti.it	03715941
Rappresentante del titolare	N/A		
Responsabile protezione dati (DPO)	Z Holding Spa	dpo@zucchetti.it	03715943191

DESCRIZIONE

My Whistleblowing è parte della suite My Governance, una soluzione in cloud che permette di digitalizzare i processi aziendali.
In particolare, My Whistleblowing 2.0 permette la gestione del processo di segnalazione di illeciti da parte sia di dipendenti sia dei collaboratori/utenti esterni dell'azienda. garantisce la riservatezza delle informazioni ivi inserite, nonché, di effettuare segnalazioni in forma anonima.

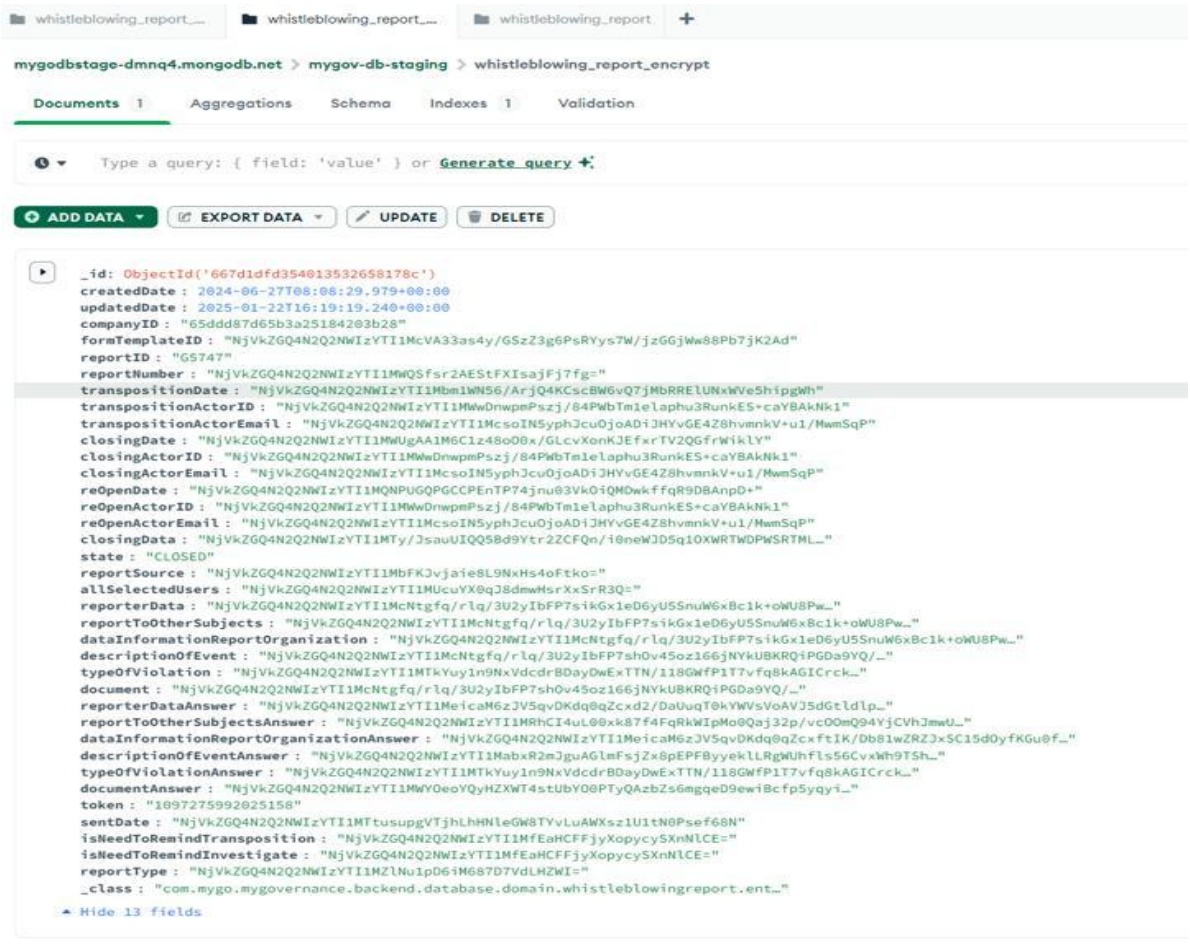
E' un'applicazione cloud (SaaS) accessibile con qualunque dispositivo senza necessità di installazione di software/app aggiuntivo con un'interfaccia estremamente semplice.
L'Architettura separa funzionalmente gli ambienti separando le due figure chiave: Segnalante e Gestore delle segnalazioni.
(per ulteriori specifiche relativamente ai due ambienti, cfr. di seguito "Misure di sicurezza implementate nei sistemi").

My WB 2.0 consente al segnalante, a seconda della configurazione, di scegliere tra due modalità di accesso distinte (alternative o non):

- Accesso anonimo tramite Token

- Accesso personalizzato tramite Login/Password (Modulo PWD)* → registrazione dell'account.

Indipendentemente dalla configurazione acquistata, se il segnalante decide di accedere in modalità anonima col token, utilizzerà il token presente all'interno della piattaforma My Governance che costruirà un codice di 16 cifre, univoco e generato in forma casuale.
Il codice viene memorizzato in una tabella in cui tutti gli altri campi sono criptati, quindi non è riconducibile a nessun utente. Di seguito prova della garanzia dell'anonimato



Ad esso non viene collegato (e memorizzato) alcun campo aggiuntivo come ip o device, al fine di mantenere il tutto effettivamente anonimo, tantochè è onere del segnalante memorizzarsi il codice creato, poichè a quel codice corrisponde solo una (e quella) segnalazione, nonché ricordarsi di controllare l'andamento della segnalazione poiché non riceverà alcuna notifica dal sistema.

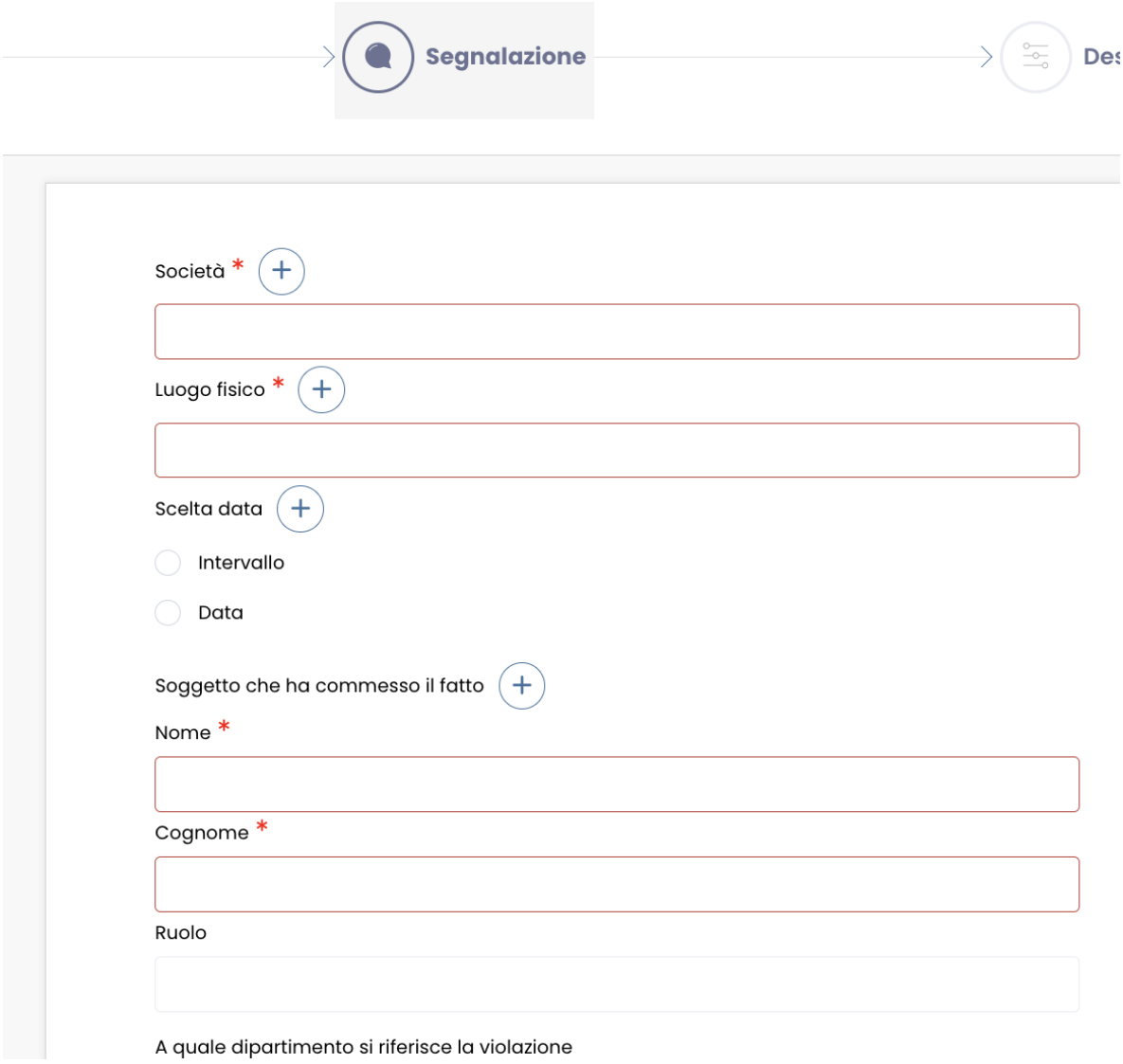
Inoltre, sempre a seconda della configurazione scelta dal Cliente (anche a fronte della procedura aziendale), MY WB 2.0 consente ai segnalanti di scegliere 3 diverse modalità di segnalazione:

- Segnalazione scritta
- Segnalazione vocale/orale (opzionale)

- Segnalazione in presenza/calendarizzazione incontro (opzionale).

Il sistema garantisce sempre che la gestione delle segnalazioni e la comunicazione tra Segnalante e Gestore rispettino i requisiti di riservatezza e anonimato (ovviamente se l'accesso è avvenuto mediante registrazione); nel caso di accesso con token si è confermato l'anonimato sopra.

Ulteriore garanzia di riservatezza è garantita dal fatto che anche all'interno della segnalazione gli unici campi che obbligatoriamente devono essere compilati sono "Società", "Luogo fisico", "Nome" e "Cognome" del segnalato, come da screensho di seguito:



Infine, indipendentemente dalla modalità di accesso è confermato e garantita la criptazione di tutti i dati della segnalazione (anche personali se presenti) oltre agli allegati (come ulteriormente specificato in "*Categorie di dati personali"* trattati e in "*Misure di sicurezza implementate nei software*").

My Whistleblowing 2.0 prevede 2 configurazioni di licenza:

- Flex
- Smart

La differenza principale tra le due licenze è che il primo ("Flex") permette personalizzazioni e attivazione di moduli aggiuntivi a differenza del secondo che non le permette.

In via esemplificativa "Flex" permette la personalizzazione della segnalazione (in base alla procedura whistleblowing aziendalmente costruita); la possibilità di differenziare le categorie di illeciti oggetto di segnalazione al fine che siano gestite dal Gestore maggiormente competente in materia …

Entrambi invece prevedono la creazione di report tabellari di sintesi che documentano, per ogni segnalazione, i dati relativi alla gestione delle istruttorie.

FINALITA' DEL TRATTAMENTO

Il Responsabile del trattamento tratta i dati per finalità di creazione utenza, assistenza e manutenzione al Titolare. Si fa presente che il Responsabile non ha accesso alle informazioni contenute all'interno della singola segnalazione, che restano pertanto accessibili esclusivamente al Titolare

CATEGORIA INTERESSATI

Dipendenti, apprendisti, tirocinanti, stagisti, collaboratori, fornitori, appaltatori, visitatori, Gestori a seconda della scelta del Cliente su chi avrà accesso alla piattaforma My Whistleblowing.
Inoltre sono presenti i dati dei soggetti segnalati, nonché di potenziali testimoni (i quali, in quanto parte della segnalazione sono protetti sempre da crittografia).

CATEGORIE DI DATI PERSONALI

Nel caso di accesso alla segnalazione mediante registrazione: unico dato trattato è l'indirizzo e-mail, richiesto obbligatoriamente per costruire l'"account segnalante" con cui poi creerà le segnalazioni. Potenzialmente anche nome e cognome, a discrezione dell'utente nel fornirli.

Nel caso di accesso con Token non si tratta alcun dato personale.

Relativamente al segnalato, sono presenti nome e cognome, a cui sono collegate le informazioni oggetto di segnalazione (ad esempio dati dei testimoni, se presenti).

Si ricorda che il Responsabile non ha accesso ai dati personali rilasciati all'interno della singola segnalazione, poiché protetta da crittografia., indipendentemente dalla modalità di accesso del segnalante.

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

Aziende del gruppo Zucchetti
Subappaltatori
Amazon Web Service EMEA SARL come provider di DC
MongoDB, come Database.
PAR-TEC S.p.A. quale partner fornitore di attività di assistenza sistemistica estesa H24

TRASFERIMENTO DATI ALL'ESTERO

No

TERMINI PER LA CANCELLAZIONE DEI DATI

Il sistema è programmato affinché dopo 5 anni, dalla chiusura della segnalazione, questa e i documenti relativi vengano cancellati, come previsto normativamente.

In ogni caso i dati conservati nel Data Center fornito in cloud da AWS saranno conservati per tutta la durata del contratto e successivamente, per il tempo e nelle modalità stabilite contrattualmente col Cliente oppure su richiesta del Titolare, potranno essergli consegnati con una estrazione unica entro 30 giorni dalla fine del contratto. In ogni caso le misure adottate per tutelare la riservatezza della segnalazione restano anche con l'estrazione, perciò le segnalazioni saranno consegnate criptate e anonime. Dopo di che verranno distrutti all'interno del nostro database con tempi da concordare.
I dati relativi alla gestione amministrativa e giuridica del rapporto contrattuale saranno conservati per 10 anni dalla cessazione del rapporto contrattuale.

ZUCCHETTI

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza già implementate o configurabili nel sistema applicativo sono:

- *Separazione ambienti "Segnalante" e "Gestore delle segnalazioni":*

Ambiente e macrofunzioni Segnalante	**Ambiente e macrofunzioni Gestore**
Il sistema garantisce la completa riservatezza dei dati del segnalante e della segnalazione, separando il contenuto della segnalazione dall'identità del Segnalante (nel caso il Segnalante accedesse con registrazione e non con il token. Nel caso di accesso con Token è garantita l'anonimato come sopra maggiormente descritto).	La funzione Gestore dispone di un'area riservata per la gestione delle segnalazioni, che consente la qualificazione, l'istruttoria e la storicizzazione delle segnalazioni
L'interfaccia è intuitiva e si adatta ai diversi livelli di alfabetizzazione del segnalante, che dispone di un'area privata per la segnalazione e per monitorare lo stato di avanzamento dell'istruttoria	L'applicazione consente la comunicazione diretta tra Gestore e Segnalante per consentire a Gestore l'integrazione delle informazioni utili a completare l'istruttoria
Il Segnalante ha sempre modo di integrare e aggiornare i dati delle segnalazioni, integrando le informazioni anche con documenti multimediali	Il Gestore può richiedere contributi alle diverse funzioni di controllo delegate: l'applicazione consente l'operatività dei diversi gestori in forma collaborativa, in modo tale da facilitare la gestione collegiale della segnalazione.

- *Gestione delle segnalazioni:*

- Le segnalazioni trasmesse dal Segnalante sono registrate nel sistema e non sono cancellabili;

- I dati e i documenti relativi alle istruttorie delle singole segnalazioni non possono essere modificati una volta chiusa l'istruttoria;
- Il sistema, in base alla norma, prevede un'archiviazione massima di 5 anni;
- Un automatismo di cancellazione si attiva alla scadenza del quinto anno dalla data della comunicazione dell'esito finale delle procedure di segnalazione;
- il sistema è dotato di notifica via e-mail al Gestore all'avvicinarsi della scadenza;
- il workflow della segnalazione è preconfigurato in base alla licenza acquistata.

  - *Gestione profili e credenziali di accesso:*

- A seconda della configurazione, consente al Segnalante di scegliere tra 2 diverse modalità di accesso:
  - Accesso anonimo tramite Token
  - Accesso personalizzato tramite Login/Password (Modulo PWD)*
- A prescindere dalle modalità di accesso, al Segnalante viene assegnato un profilo di utente univoco, che consente l'accesso ad un'area personalizzata entro cui può:
  - Accedere alla segnalazione precedentemente storicizzata nel sistema
  - Visualizzare gli aggiornamenti dello stato istruttoria e le notifiche dei messaggi
  - Partecipare alle chat collaborative con Gestore
  - Accedere alla segnalazione in modifica/aggiunta informazioni e documenti
  - Creare il report di una nuova segnalazione, in modalità anonima o nominativa
- Ai Gestori possono essere assegnati profili differenziati, caratterizzati da differenti permessi di accesso alle segnalazioni, in base a:
  - *profilo di competenza*: l'accesso alle diverse tipologie di segnalazioni può essere definito secondo logiche di competenza funzionale;
  - *profilo di operatività*: il Gestore può accedere alle segnalazioni in modalità:
    - *Modifica*. Questo profilo consente l'aggiunta di informazioni e documenti, la gestione delle chat con Segnalante e gli altri gestori, la gestione stati istruttoria
    - *Sola consultazione* dei report delle segnalazioni.
- A ogni gestore viene assegnato un profilo di utente univoco, che consente l'accesso tramite login/password ad un'area personalizzata entro cui potrà accedere ai report e gestire le segnalazioni secondo competenza.
- *User name*: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Ogni gestore/amministratore di sistema è collegato ad una singola utenza assegnata univocamente. Le utenze (anche amministrative) sono nominali e non condivise, al fine di evitare la possibilità che soggetti non autorizzati possano operare in assenza di specifica volontà del titolare. Il soggetto coinvolto nel trattamento riceverà un codice identificativo ("User ID") associato ad una parola chiave ("password") secondo i migliori standard attualmente in commercio.

- Password: password con requisiti minimi di sicurezza garantiti. Le regole di complessità della password sono quelli standard secondo le best practice di settore (minimo 16 caratteri, almeno una maiuscola, una minuscola, un carattere speciale e un numero). La password di accesso al software deve essere cambiata ogni 90 giorni, con una password diversa dalle tre precedenti dello storico.
- Criteri di complessità per le impostazioni delle credenziali: le credenziali di accesso possono essere impostate secondo diversi criteri di complessità dal Titolare.
- Il Sistema prevede la funzione di blocco account a tempo oppure il blocco account per superamento tentativi di login fail: al terzo tentativo errato di immissione di una password, l'utente verrà bloccato per 30 minuti.
- È possibile implementare una two factor authentication anche attraverso un sistema di otp o codice numerico inviato via e-mail.

  - *Minimizzazione:*

- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti, in particolare nella individuazione admin/user.
- Conservazione della segnalazione (e della relativa documentazione) per il tempo stabilito dalla norma.
- (solo nella versione ""Flex") Il sistema permette l'attivazione di una specifica funzionalità a livello applicativo che consente al Gestore delle segnalazioni di archiviarle applicando differenti policy di data retention fermo restando le limitazioni di legge.

  - *Identificazione di chi ha trattato i dati:*

  L'architettura dell'applicazione non consente l'integrazione con applicazioni esterne così come il tracciamento mediante log dell'accesso all'applicativo, al fine di tutelare la riservatezza dell'identità dei segnalanti anche in caso di utilizzo della rete aziendale. Il sistema prevede solo il tracciamento dei file di log relativi alle modifiche dei dati: offre infatti la possibilità di tracciamento del log di tutti gli utenti che hanno effettuato l'ultima modifica alla segnalazione. Il log può essere estrapolato su richiesta facendo riferimento all'arco temporale desiderato (massimo 12 mesi).

  - *Tecniche di crittografia:*

  L'intero ciclo di gestione dei dati viene crittografato utilizzando l'algoritmo di crittografia AES256 (Crypting protocol: "Advanced Encryption Standard" (lo stesso che usa il governo USA) AES / CBC / NOPADDING). Durante la comunicazione "in transito" tramite TLS / Protocolli HTTPS. Tutto lo spazio di archiviazione è crittografato AES256 e i dati sensibili sono crittografati nel database, si hanno:
    - Crypting password DB service account.
    - Crittografia della base dati: Il database è crittografato secondo gli standard di servizio offerti da mongoDB atlas: https://www.mongodb.com/products/capabilities/security/encryption.

- Crittografia file DMS: tutti i documenti generati dalle applicazioni e conservati nel DMS sono crittografati; la crittografia per eventuali documenti generati all'esterno e archiviati nel DMS, verrà applicata impostando correttamente i parametri sulla "Classe documentale" associata ai documenti stessi.

- *Privacy by default*

- Attivazione profilo utente: gli utenti nel portale sono attivati secondo una logica di non assegnare alcun profilo autorizzativo sui dati trattati. Sarà il Titolare in autonomia a scegliere la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale. In particolare, il Titolare potrà individuare la funzione admin, ruolo che consente di verificare le segnalazioni ricevute. Tale funzione viene assegnata o a un singolo ricevente, ovvero a un comitato di riceventi, a seconda delle necessità del Titolare.
- Conservazione della segnalazione (e relativa documentazione) per 5 anni (come da norma vigente) a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

- *Diritti degli interessati:*

- Diritti degli interessati: per garantire agli interessati il diritto all'oblio, nei limiti di quanto permesso, è sufficiente che inviino una richiesta al Titolare che potrà informare il Responsabile per provvedere alla cancellazione. Per la precisione, si potrà ottenere la cancellazione dei dati solo se non è collegata all'utenza alcuna segnalazione. In caso contrario si dovranno attendere i termini legali di cancellazione automatica della segnalazione e quindi, poi, la possibilità di cancellazione dei propri dati personali. Nel caso di accesso con token non si è in presenza di dati personali, pertanto, la richiesta di cancellazione non può sussistere.

ULTERIORI MISURE DI SICUREZZA

Misure di sicurezza	Commenti
Mettere in sicurezza lo stabile che ospita l'infrastruttura IT utilizzata per elaborare e trasferire i dati	I dati della piattaforma My Governance sono conservati sui server Europei di AWS.
Limitare il numero di soggetti autorizzati ad accedere ai dati e all'infrastruttura IT utilizzata per elaborare e trasferire i dati	La società che fa manutenzione alla piattaforma è stata debitamente individuata come Amministratore di Sistema. L'accesso fisico ai data center AWS viene registrato, monitorato e conservato. L'accesso fisico è controllato ai punti di ingresso dell'edificio da personale di sicurezza professionale che utilizza sistemi di sorveglianza, rilevamento e altri mezzi elettronici. Il personale autorizzato utilizza meccanismi di autenticazione a più fattori per accedere ai data center. Gli ingressi alle sale server sono protetti con dispositivi che emettono allarmi per avviare una risposta a un incidente se la porta viene forzata o tenuta aperta. I sistemi elettronici di rilevamento delle intrusioni sono installati all'interno del livello dati per monitorare, rilevare e avvisare automaticamente il personale appropriato di incidenti di sicurezza. I punti di ingresso e di uscita verso le sale server sono protetti con dispositivi che richiedono a ciascun individuo di fornire l'autenticazione a più fattori prima di concedere l'ingresso o l'uscita. Questi dispositivi emetteranno allarmi se la porta viene forzata aperta senza autenticazione o tenuta aperta. I dispositivi di allarme porta sono inoltre configurati per rilevare le istanze in cui un individuo esce o entra in un livello dati senza fornire l'autenticazione a più fattori.
Assicurare un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza	Grazie alla società terza che garantisce la continuità del Data Center (DC) si assicurerà un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza
Assicurare che l'accesso ai dati avvenga in maniera controllata	L'accesso ai dati può avvenire solo in maniera controllata, grazie agli alti standard di sicurezza con cui viene protetto il DC e alla criptazione dei dati.

	L'accesso fisico al data center è fornito solo ai dipendenti autorizzati. Tutti i dipendenti che necessitano dell'accesso al data center devono prima richiedere l'accesso e fornire una giustificazione aziendale valida. Queste richieste vengono concesse in base al principio del privilegio minimo, in cui le richieste devono specificare a quale livello del data center l'individuo deve accedere e sono limitate nel tempo. Le richieste vengono esaminate e approvate da personale autorizzato e l'accesso viene revocato allo scadere del tempo richiesto. Una volta concessa l'ammissione, le persone sono limitate alle aree specificate nelle loro autorizzazioni.
Assicurare che i dati siano protetti da perdita o distruzione accidentale	Per assicurare che i dati siano protetti da perdita o distruzione accidentale si utilizzano copie di backup dislocate in posizioni geografiche differenti. Tale livello di protezione ridurrà al minimo la possibilità di perdita e comunque nel caso dovesse avvenire sarà sicuramente molto limitata.
Anonimizzazione	Il sistema separa logicamente i contenuti del database in modo tale per cui i dati delle segnalazioni risultano separati dai dati del segnalante. Senza esplicita volontà del segnalante non è mai possibile associare una segnalazione al ID di un segnalante
Assegnare credenziali di autenticazione univoche	Ogni soggetto coinvolto nel trattamento avrà assegnate credenziali di autenticazione composte da un codice per l'identificazione ("User ID") associato a una parola chiave ("password") secondo gli standard migliori oggi presenti sul mercato. Password con sicurezze minime garantite
Garantire complessità della password	La password di accesso dovrà rispettare quantomeno i seguenti requisiti: ● almeno 16 caratteri ● almeno una lettera maiuscola ● almeno una lettera minuscola ● almeno un simbolo speciale ● almeno un numero Al terzo tentativo errato di inserimento di una password l'utenza verrà bloccata per 30 minuti. La password di accesso al software deve essere cambiata ogni 90 giorni, con una password diversa

	dalle tre precedenti dello storico.
Assicurare che lo User ID assegnato ad un Utente non possa essere assegnato ad un altro incaricato in tempi diversi	Questo deve essere garantito dal Titolare in quanto lo user ID è l'indirizzo email
Assicurare che: i. quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso venga utilizzato un sistema di autorizzazione. ii. i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, siano individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. iii. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	Confermato Con l'assunzione vengono resi disponibili i documenti di sistema per la nuova risorsa e più precisamente: - la politica di sicurezza delle informazioni; - la disciplina sul corretto utilizzo degli strumenti assegnati al fine di non compromettere la sicurezza delle risorse aziendali; - le procedure e le istruzioni relative al ruolo e ai compiti - sottoscrizione di accordo di riservatezza
Proteggere i dati dal rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale: i. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza quotidiana; ii. effettuare aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti su base quotidiana	Confermato Per la valutazione delle vulnerabilità dei sistemi: - si può avvalere di consulenti esterni individuati allo scopo di effettuare test di penetrazione (con frequenza almeno biennale), ovvero utilizzando software ad hoc che effettueranno test di vulnerabilità automatici su base ricorrente; - ha implementato un processo di monitoraggio delle vulnerabilità e ha adottato una policy di patch che prevede la fornitura di patch di sicurezza periodiche, infine implementate anti-malware sui componenti; - permette al Cliente di condurre test di penetrazione, valutazioni di vulnerabilità e sopralluoghi presso le sedi.
Assicurare che il trattamento avvenga utilizzando software (ivi incluso il sistema operative, il middleware e le applicazioni) dotati di funzioni di sicurezza all'avanguardia	Confermato
Assicurare che sia effettuato un back-up almeno con	Grazie alla società terza proprietaria dei server si

frequenza quotidiana	assicurerà che sia effettuato un back-up almeno con frequenza quotidiana. Si possono distinguere 3 tipi di backup: infrastruttura, database e storage.
Assicurare che i dati possano essere recuperati entro un determinato termine massimo (non più di 7 giorni)	Sì è presente un piano di Business Continuity e Disaster Recovery
Garantire che i dati utilizzati per l'autenticazione siano protetti con efficaci misure di sicurezza crittografica	Sì
Assicurarsi che i dati trasferiti siano protetti utilizzando procedure di crittografia aggiornate	Sì Sono utilizzate le applicazioni di mongoDB atlas: https://www.mongodb.com/products/capabilities/security/encryption
Le categorie particolari di dati personali sono protette utilizzando procedure di crittografia aggiornate	Normalmente non vengono trattate categorie particolari di dati personali ma in ogni caso i dati in nostro possesso sono sempre crittografati
Assicurarsi che sia possibile verificare e stabilire se e chi ha avuto accesso o ha inserito, ha modificato o cancellato i dati nei sistemi di elaborazione dati. I log devono essere disponibili per almeno un anno	Confermato
Garantire che siano regolarmente eseguiti test di vulnerabilità e di penetrazione	Cadenza annuale (da soggetti esterni) o su base ricorrente mediante software ad hoc
Qualora una violazione o vulnerabilità sia identificata nell'ambito del trattamento o in qualsiasi sistema utilizzato per fornire i servizi del Responsabile, informare immediatamente il Titolare del trattamento in merito all'evento e alle misure adottare per porvi rimedio	Sì è presente una policy di gestione incidenti
Garantire che l'accesso ai dati sia limitato ai soli dati necessari per effettuare le operazioni di trattamento.	Sì by default
Limitare il numero di Incaricati autorizzati a svolgere attività connesse al trattamento dei dati	Sì by default
Erogare apposita formazione nei confronti degli Incaricati con riferimento alla normativa vigente in materia di tutela dei dati personali, alle misure di sicurezza	Sì E' prevista un'adeguata formazione sulla Cyber Security, al fine di garantire che tutto il personale sia informato sui rischi per la sicurezza incorsi nell'utilizzo delle risorse aziendali e adeguatamente formato per consentire allo stesso di riconoscere situazioni di potenziale e/o concreta minaccia per la sicurezza. Viene inoltre svolta una formazione specifica per i rischi di cybersecurity come quelli legati al phishing e tutte le problematiche connesse al GDPR.

	Il programma di formazione è costruito e adattato ai diversi ruoli e compiti svolti in azienda. L'efficacia di tale programma è verificata periodicamente, e comunque almeno annualmente, al fine di intraprendere le necessarie azioni correttive e/o integrarlo alle nuove esigenze conoscitive che possono sorgere.
Mantenere una lista aggiornata degli Incaricati	Presente
Mantenere una copia di riserva aggiornata dei dati e del software utilizzato per il trattamento	Presente
Garantire che i Dati vengano archiviati applicando misure idonee a proteggerli da accessi non autorizzati, modifiche, danni e distruzione	Presente
Assicurarsi che i dati vengano cancellati in modo irreversibile in caso di sostituzione o riutilizzo dell'hardware	Sì by default Al termine del rapporto di lavoro l'ufficio informatico, tempestivamente informato dalla funzione HR, provvede al ripristino dei dispositivi aziendali assegnati a ciascun dipendente e alla chiusura/cancellazione dei profili/utenti in nome dello stesso. Sono definite adeguate procedure per la restituzione dei beni (es. computer portatili, cellulari, documenti, software, manuali, carte di credito) assegnati al personale che ha cessato il rapporto di lavoro.
Escludere o limitare le copie dei dati (incluse le stampe) e assicurare la corretta distruzione dopo l'utilizzo	Sì by default
Proteggere i documenti cartacei contenenti dati utilizzati durante l'elaborazione al momento della stampa, archiviazione, distruzione e scambio	Non viene utilizzato alcun documento cartaceo
Garantire la sicurezza della rete su cui viene eseguito il trattamento (sistema firewall, proxy, sistemi di rilevamento delle intrusioni o altri dispositivi attivi o passivi)	Presente ✓ monitora il traffico sulle proprie reti e sui sistemi informatici al fine di rilevare possibili attacchi alla sicurezza informatica e interruzioni del sistema e informa il personale; ✓ mantiene registri ed effettuare prove adeguate per consentire l'indagine sugli incidenti e preserva la custodia di tali dati, anche per procedimenti giudiziari o di prova;

	✓ ha una procedura di gestione dell'incidente (Rilevamento, classificazione, inizio indagine e contenimento, risoluzione incidente, chiusura dell'incidente, creazione di un quadro per risoluzione di incidenti simili e valutazione del quadro)

Queste misure di sicurezza devono essere correttamente impostate da parte del Titolare.

2. MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA DI PRIMO LIVELLO

ASSISTENZA ON SITE

Gli addetti Zucchetti offrono al Titolare formazione e sono disponibili a recarsi anche on site per eventuali supporti, ferma restando l'assistenza continua da remoto secondo gli SLA condivisi con il cliente.
In questo caso gli addetti My Governance lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezza implementate dallo stesso. I Titolari potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere in affiancamento per formare il loro personale.
Qualora durante l'attività di assistenza l'addetto My Governance abbia la necessità di prelevare archivi o db di cui necessita per risolvere le problematiche evidenziate è necessario che informi il Titolari e registri tale attività sulla Nota di intervento..

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite email i tecnici Zucchetti rendono sempre disponibile tramite link la possibilità per Titolare di leggere l'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.
L'addetto Zucchetti non è autorizzato a farsi mandare le credenziali di accesso del Titolare via email né tantomeno potrà salvarle sullo strumento di ticketing.
Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico My Governance è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico My Governance dovrà richiedere credenziali individuali oppure collegamento tramite strumenti a ciò dedicati.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO SU IP PUBBLICI OPPURE TRAMITE VPN

Qualora l'attività di assistenza debba essere svolta su sistemi cloud su IP pubblici oppure tramite VPN o accessi privati è necessario che gli addetti Zucchetti entrino nei sistemi dei Titolari:

- Previa autorizzazione del cliente
- Previa ricezione delle credenziali individuali e le stesse siano state attivate per il tempo necessario all'esecuzione delle attività richieste
- al termine dell'attività siano disattivate le credenziali da parte del Titolare

Personale di Help Desk

La creazione dell'utenza deve essere richiesta solo al Titolare che, attraverso l'amministratore di applicazione, potrà creare il nuovo utente.
Non deve mai essere utilizzato l'utente amministratore da parte degli operatori di assistenza.

3 MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS e AL DATA CENTER

Zucchetti pone i propri sistemi sul server certificato di AWS.
Relativamente ai servizi offerti da AWS, di seguito ulteriori specifiche:
- ***BACKUP:*** si distinguono tre diversi tipi di backup: infrastruttura, database e storage.
  - Infrastruttura: tutti i server utilizzati per eseguire la nostra applicazione
  - Database: contiene tutti i dati visualizzati sull'applicazione
  - Server di archiviazione: contiene tutti i file visualizzati sull'applicazione.

- *ZONE DI DISPONIBILITÀ*: Una zona di disponibilità è un data center logico in una regione disponibile per l'utilizzo da parte di qualsiasi infrastruttura AWS.
Ogni zona di una regione dispone di alimentazione, rete e connettività ridondanti e separate per ridurre la probabilità che due zone si guastino contemporaneamente. Ci sono tre AZ (Availability Zone) nella regione di Francoforte. Se uno dei nodi dell'infrastruttura si interrompe, gli altri 2 sono in esecuzione.

- *SICUREZZA PIATTAFORMA*: la piattaforma risiede su Amazon Virtual Private Cloud (VPC – nella fattispecie AWS EC2), ma con tecnologia Serverless (Fargate), pertanto la responsabilità è di AWS.

1) ECS Fargate {Serverless): AWS Fargate soddisfa la conformità ai fini PCI DSS Level 1, ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3 e HIPAA.
Come servizio gestito, Amazon Elastic Container Service è protetto dalle procedure di sicurezza della rete globale di AWS.
L'utilizzo di ECS con i servizi Fargate non viene eseguito direttamente su un sistema operativo che può causare vulnerabilità alla nostra applicazione web.
Il codice della nostra applicazione viene verificato a livello di sviluppo prima di essere inviato alla finestra mobile; quindi, la protezione antivirus è una preoccupazione per gli sviluppatori della nostra applicazione web.
Poiché la nostra infrastruttura utilizza effettivamente immagini docker, i nostri sviluppatori verificano il codice prima di eseguire il commit.

2) Cloudflare Security Services:: offre le seguenti funzionalità:

Protezione DDoS avanzata per servizi e applicazioni esposte su Internet
Cloudflare fornisce una protezione DDoS always-on attraverso la propria rete globale distribuita, monitorando e analizzando in tempo reale il traffico in ingresso. I meccanismi di rilevamento basati su analisi comportamentale, threat intelligence e identificazione delle anomalie consentono di individuare e mitigare automaticamente attacchi volumetrici e tentativi di saturazione delle risorse, garantendo la continuità operativa dei servizi pubblicati.

Mitigazione degli attacchi in linea
Le funzionalità di mitigazione sono integrate nativamente nell'infrastruttura Cloudflare e vengono applicate in linea senza impatti significativi sulle prestazioni. Il traffico malevolo viene identificato e filtrato attraverso tecniche di rate limiting, traffic shaping, challenge automatici, reputazione degli

indirizzi IP e analisi del comportamento delle richieste. La protezione copre sia gli attacchi di rete (Layer 3 e 4) sia gli attacchi rivolti al livello applicativo (Layer 7).

Web Application Firewall (WAF) e protezione OWASP Top 10

Cloudflare integra un Web Application Firewall (WAF) con regole gestite e continuamente aggiornate per la protezione delle applicazioni web. Il servizio consente di prevenire e mitigare le principali vulnerabilità applicative individuate dall'OWASP Top 10, tra cui SQL Injection (SQLi), Cross-Site Scripting (XSS), Remote Code Execution (RCE), Path Traversal e altre minacce rivolte ai servizi web. Le richieste HTTP/HTTPS vengono analizzate in tempo reale e bloccate prima di raggiungere i sistemi esposti.

Protezione da bot e controllo degli accessi automatizzati

Cloudflare include funzionalità di identificazione e gestione del traffico automatizzato che consentono di mitigare attività malevole generate da bot, crawler non autorizzati e tentativi di abuso delle applicazioni. Tali funzionalità contribuiscono alla protezione delle risorse applicative da attività fraudolente, scansioni automatiche e tentativi di sfruttamento delle vulnerabilità.AWS Shield Standard fornisce un monitoraggio del flusso di rete sempre attivo che ispeziona il traffico in entrata ai servizi AWS e applica una combinazione di firme del traffico, algoritmi di anomalia e altre tecniche di analisi per rilevare il traffico dannoso in tempo reale. Shield Standard imposta soglie statiche per ogni tipo di risorsa AWS, ma non fornisce alcuna protezione personalizzata alle applicazioni dei clienti AWS.

3) Cloudflare Web Application Firewall (WAF): Cloudflare WAF è un firewall applicativo cloud-native che consente di monitorare, filtrare e proteggere il traffico HTTP(S) diretto alle applicazioni web pubblicate su Internet.

Sono state abilitate regole di sicurezza gestite e costantemente aggiornate, basate sulle migliori pratiche di settore e sulle vulnerabilità identificate dall'OWASP Top 10, al fine di proteggere le applicazioni web dai principali vettori di attacco, tra cui:

A01 - Broken Access Control

A02 - Cryptographic Failures (Sensitive Data Exposure)

A03 - Injection (SQL Injection, Command Injection, ecc.)

A04 - Insecure Design

A05 - Security Misconfiguration

A06 - Vulnerable and Outdated Components

A07 - Identification and Authentication Failures

A08 - Software and Data Integrity Failures

A09 - Security Logging and Monitoring Failures

A10 - Server-Side Request Forgery (SSRF)

Il servizio analizza in tempo reale le richieste HTTP(S) e applica controlli di sicurezza finalizzati all'identificazione e al blocco di traffico malevolo, tentativi di sfruttamento delle vulnerabilità applicative, scansioni automatiche e attività riconducibili a bot dannosi.

Cloudflare WAF integra, inoltre, funzionalità avanzate di Rate Limiting, Bot Protection, IP Reputation Filtering e regole personalizzabili, consentendo di adattare la protezione alle specifiche esigenze dell'applicazione e del contesto operativo.

La piattaforma mette a disposizione dashboard centralizzate per il monitoraggio degli eventi di sicurezza, la visualizzazione delle metriche di traffico, l'analisi dei tentativi di attacco e la gestione delle policy di protezione, garantendo piena visibilità e controllo sullo stato di sicurezza delle applicazioni esposte.

- ***INFRASTRUTTURA DI BACKUP E RIPRISTINO***

Sono presenti 3 zone di disponibilità, quindi 3 data center ridondanti.
E' prevista comunque una procedura di ripristino, le cui specifiche sono fornite su richiesta.
In ogni caso per il ripristino del DB si utilizza il servizio cloud Mongo Atlas, che garantisce di rispettare i tempi di RPO ed RTO.
Come storage si utilizza Amazon S3.

Per ulteriori informazioni tecniche relativamente ai servizi offerti da AWS si rimanda ai seguenti link

- https://aws.amazon.com/it/legal/
- https://aws.amazon.com/it/compliance/
- https://aws.amazon.com/it/s3/
- https://aws.amazon.com/it/backup/.