[English version below]

Norme sulla privacy relative alle APP Zucchetti

resa ai sensi dell'art. 13 Regolamento Europeo per la protezione dei dati personali 2016/679 (GDPR)

La presente Informativa Privacy è resa solo ed esclusivamente per l'applicazione Zucchetti **ZSafe PRO MED** e non anche per eventuali siti web attraverso i quali ad esempio l'Utente dovesse accedere a / o utilizzare l'applicazione.

Titolare del Trattamento

Titolare del trattamento dei dati personali, ai sensi dell'art. 4 punto 7 del GDPR, è Zucchetti S.p.A. con sede legale in Lodi, Via Solferino, n. 1, 26900 – e-mail ufficio.privacy@zucchetti.it

Responsabile della protezione dei dati

Il responsabile per la protezione dei dati è il dott. Mario Brocca a cui potrà rivolgersi scrivendo una email a dpo@zucchetti.it

Sviluppatore

Lo Sviluppatore dell'applicazione è InfoFactory S.r.l., con sede legale a Udine, Via Jacopo Linussio 51, Udine 33100 - persona di riferimento Massimiliano Valotto valotto@infofactory.it

Dati personali raccolti

I servizi forniti dalla App, nonché le caratteristiche e le funzioni della stessa non richiedono alcuna forma di registrazione degli Utenti. Segnaliamo tuttavia che, i sistemi informatici e le procedure software preposte al funzionamento della App (come ad esempio Apple Store o Google Play), acquisiscono nel corso del loro normale esercizio, alcuni dati comunque riferibili all'Utente la cui trasmissione è implicita nell'uso dei protocolli di comunicazione internet, degli smartphone e dei dispositivi utilizzati. In questa categoria di dati rientrano, a titolo esemplificativo ma non esaustivo, la posizione geografica, l'identità del telefono, i contatti dell'Utente, e-mail, i dati relativi alla carta di credito.
L'Utente potrà consultare le informazioni sulla Privacy disponibili sui seguenti siti:

- Apple Store- http://www.apple.com/legal/privacy/it/
- Google Play- https://www.google.it/intl/it/policies/privacy/

L'app **ZSafe PRO MED** raccoglie i seguenti dati personali:

- **fotocamera** per leggere una combinazione di dati all'interno di un QR code per configurare l'app, per proporre automaticamente i dati in fase di compilazione, e per l'acquisizione di eventuali documenti da registrare nella cartella sanitaria e di rischio del lavoratore. Le immagini vengono salvate in una locazione di memoria del telefono non accessibile all'utente al di fuori dell'app. Le immagini acquisite come allegati vengono inviate al server che le storicizza nel Document Management System e possono essere eliminate in qualsiasi momento dal cliente.
- **microfono**: eventualmente utilizzato solo dalla tastiera virtuale del dispositivo. Non vengono salvati dati nell'app
- **dati biometrici**: la gestione della biometria viene effettuata direttamente dal produttore del device all'interno dello stesso; pertanto, Zucchetti, in qualità di produttore dell'applicazione, non conosce né dove né le modalità con cui i dati biometrici sono salvati sul device e non può accedervi. L'unica attività che viene effettuata da Zucchetti è quella di interrogare il sistema operativo per chiedere la validazione delle credenziali biometriche, che potranno essere dallo stesso confermate o meno senza alcuna visibilità sul processo e sui dati biometrici sottostanti.
- **username, password e url** di collegamento necessari per accedere alle funzionalità dell'app;
- **anagrafica del lavoratore** (cognome e nome, sesso, luogo di nascita, data di nascita, domicilio, nazionalità, codice fiscale, mansione inquadramento aziendale);
- **dati relativi al rapporto di lavoro** e inquadramento contrattuale, mansione, documentazione necessaria per la gestione del rapporto (p. es. carte di identità, formazione);
- **dati relativi allo stato di salute del lavoratore** e/o dei propri familiari (visita preventiva, anamnesi lavorativa, anamnesi familiare, anamnesi fisiologica, anamnesi patologica remota, anamnesi patologica prossima, esame

obiettivo (con particolare riferimento agli organi bersaglio), accertamenti integrativi, eventuali provvedimenti del medico competente, giudizio di idoneità alla mansione specifica).

Natura obbligatoria o facoltativa del conferimento dei dati e conseguenze di un eventuale rifiuto

Il conferimento dei dati è facoltativo ma sono necessari per l'erogazione del servizio. Il rifiuto al conferimento non consente l'erogazione del servizio e l'utilizzo dell'app.

Modalità del trattamento

I trattamenti avvengono in formato elettronico e durante l'utilizzo dell'app i dati personali dei lavoratori sono reindirizzati attraverso connessioni sicure al prodotto software web HR Portal prodotto da Zucchetti. Questi dati non sono mai salvati in via definitiva sul dispositivo. L'utente (medico) può cancellarli in ogni momento utilizzando le funzioni presenti nell'app.

Procedure sicure di trattamento dei dati utente personali e sensibili

Lo sviluppatore ha sviluppato e implementato procedure sicure di trattamento dei dati costituite da misure di sicurezza a livello tecnico organizzativo, sia a livello di servizi di assistenza.

In particolare, le misure di sicurezza configurabili a livello applicativo sono:

- Gestione credenziali di accesso
  - Username: l'accesso all'App avviene previa abilitazione da parte del Titolare dei propri dipendenti/collaboratori, i quali potranno scaricare autonomamente l'App. L'accesso avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Nel sistema c'è una credenziale amministrativa che viene consegnata al titolare e da questo utilizzabile solo in circostanze eccezionali. Il titolare deve predisporre una procedura organizzativa affinché tale utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione. Nel sistema viene profilato un utente del Cliente/Titolare come Medico amministratore. Il Titolare deve predisporre una procedura organizzativa affinché tale utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione. In particolare, il Medico amministratore dev'essere abilitato all'accesso dall'amministratore di sistema (ovvero un utente appartenente al gruppo 1-Amminis. Zucchetti). L'amministratore di sistema inserisce i dati identificativi del medico, il quale riceve una notifica che lo informa che è stato designato "Medico amministratore" ai fini della gestione delle cartelle sanitarie dei lavoratori e che, per confermare la propria abilitazione, è necessario collegarsi al Portale ed inserire i propri dati identificativi. Nel caso in cui le informazioni inserite dal Medico amministratore coincidano con quelle inserite dall'Amministratore di sistema, l'abilitazione del medico è confermata e quest'ultimo può procedere all'attivazione dell'OTP per la sua utenza. Una volta che l'utenza del medico amministratore è stata abilitata, l'utente può registrare il proprio dispositivo tramite l'app mobile.
  - password: le regole di complessità della password sono configurabili nel sistema da parte del titolare. Potrà scegliere diversi gradi di complessità e applicarli a tutti gli utenti del sistema. Sono configurabili anche i tempi di sostituzione delle password.
  - criteri di complessità per le impostazioni delle credenziali
    - le credenziali di accesso possono essere impostate secondo diversi criteri di complessità dal Titolare;
    - il Cliente ha la possibilità di caricare in Blacklist Password un dizionario di password che non permette agli utenti l'inserimento di password non complesse;
    - il Cliente ha la possibilità di impostare la funzione di blocco account a tempo oppure il blocco account per superamento tentativi di login fail. Inoltre, c'è la possibilità di impostare un numero massimo di tentativi di accesso e un numero massimo di cambi password in un giorno.
  - disattivazione/disabilitazione credenziali: anche i tempi di disattivazione delle credenziali inutilizzate o la disabilitazione delle credenziali di incaricati che non hanno più le caratteristiche soggettive per accedere a quei dati personali sono configurabili nel sistema da parte del titolare;
  - per utilizzare l'app è necessario utilizzare una Two Factor Authentication attraverso un sistema di OTP.

- Minimizzazione
  - Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti. Nel dettaglio è possibile configurare i seguenti profili autorizzativi:
    - Medico amministratore, il quale ha accesso a tutte le sezioni del sistema in lettura e scrittura, ed ha la facoltà di abilitare medici all'accesso di dati sanitari;
    - Medico competente/operatore di sanità, il quale ha accesso alle sezioni dei dati sanitari in lettura e scrittura in base al profilo autorizzativo configurato dal Medico amministratore.

- Identificazione di chi ha trattato i dati
  - **Strumenti di log**: il Titolare può attivare i log della procedura con cui sono registrati gli accessi alla procedura stessa attraverso le funzionalità del Portale HR. Il log dovrà essere estratto dal Titolare e viene conservato nel sistema per 45 giorni, estendibile fino a 365 giorni in fase di configurazione;
  - **cartella sanitaria**: sulla cartella sanitaria vengono tracciate le diverse operazioni effettuate (visualizzazione, modifica, eliminazione di dati, stampa, attribuzione dei profili autorizzativi da parte del medico amministratore); il sistema registra un log criptato contenente il codice utente, il cognome ed il nome della persona che effettua la validazione e la data e l'ora in quest'ultima viene effettuata. I log non vengono cancellati;
  - **presenza di utenze di servizio per personale di assistenza**: coloro che eseguono assistenza e manutenzione sulla procedura hanno utenze nominali che dovranno essere attivate e disattivate dal Titolare in funzione della necessità.

- Tecniche di crittografia
  - **Crittografia delle password**: viene registrato un hash delle password con l'algoritmo bcrypt aggiungendo un "salt" di applicazione ed un "salt" di utente;
  - **Crypting password DB service account**;
  - **crittografia tabelle applicative**: i dati relative all'anamnesi ed all'esame obiettivo del lavoratore vengono scritti in tabelle indipendenti e crittografate; le tabelle contenenti dati sanitari sono criptate e non contengono riferimenti diretti al lavoratore cui si riferiscono; l'accesso applicativo è sempre garantito attraverso cifratura;
  - nel dispositivo mobile, **tutti i dati utilizzati in mobilità sono cifrati in un database locale**. Ogni utente registrato sull'app del singolo dispositivo ha un proprio database locale cifrato. I dati per accedere al database e al web server sono cifrati nel SecureStorage del dispositivo;
  - lo scambio dei dati tra l'app e il web server è crittografato <in application layer con tecniche di crittografia simmetrica e asimmetrica, indipendentemente da un'eventuale crittografia a livello di trasporto (HTTPS);
  - **crittografia della base dati**: È possibile crittografare il database mediante gli strumenti standard messi a disposizione dai vari DBEngine, come ad esempio TDE (Transparent Data Encryption), limitatamente ai servizi Saas e Paas e su impianti a partire dal 2006. L'opzione è attivabile solo a livello progettuale sull'hosting.
  - **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.

- Diritti degli interessati
  - **Diritti degli interessati**: per garantire agli interessati il diritto all'oblio, è sufficiente che inviino una richiesta al Titolare che farà le opportune valutazioni. Qualora il Titolare decida che i dati debbano essere cancellati potrà agire direttamente sul Portale HR, cancellando l'anagrafica all'interno di ogni applicativo dell'area HR non sarà più reperibile alcuna informazione neppure indiretta su quell'interessato. Nei singoli applicativi

saranno presenti quindi solo informazioni anonime non riconducibili neppure indirettamente ad alcun interessato. Le funzioni di cancellazione avvengono per anagrafica soggetto;

- per garantire il diritto dell'interessato di avere informazione su quali dati tratta il Titolare e alla portabilità dei suoi dati, all'interno del Portale HR c'è **la possibilità di fare delle estrazioni HTML sia della parte anagrafica che di ogni parte applicativa** che riguardano quell'interessato. Con l'HTML il Titolare potrà trasmettere i dati all'interessato che potrà trattarli per le sue finalità. Qualora l'HTML non fosse sufficiente l'esportazione potrà avvenire in XML o CSV;
- il Cliente può **anonimizzare i dati personali** degli interessati con apposite query. Questa funzione riguarda le tabelle ma non i campi note sui cui contenuti non è possibile attivare alcun controllo a livello di procedura. Il sistema è impostato con la pseudo-anonimizzazione dei dati personali rispetto all'anagrafica degli interessati. Solo i clienti che hanno scelto di gestire i collegamenti per codice fiscale non possono avvalersi di questa tecnica di protezione.

Per quanto riguarda le **procedure di assistenza**, la sicurezza del trattamento è garantita per ogni modalità di erogazione prevista con le seguenti modalità:

Assistenza On Site

Gli addetti Zucchetti accedono presso la struttura del Titolare per fare formazione od effettuare attività tecnica di manutenzione.
In questo caso gli addetti Zucchetti lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezze 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 Zucchetti 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:
Al termine dell'attività presso gli uffici Zucchetti sarà informato il Titolari sulla soluzione adottata e sulla successiva cancellazione dell'archivio.
Qualora vi fosse la necessità di conservare gli archivi per il tempo necessario al collaudo della soluzione adottata, dovrà essere informato il Titolare sul tempo massimo di conservazione di tali archivi.

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 inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'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 Zucchetti 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 Zucchetti dovrà richiedere credenziali individuali oppure collegamento tramite strumenti a ciò dedicati.
I tecnici Zucchetti firmeranno ogni email con nome e cognome e l'informazione sarà salvata nel ticketing.

Assistenza attraverso la ricezione di data base dei clienti

Qualora per risolvere il problema segnalato dal Titolare fosse necessario farsi mandare la base dati o altri files o query contenenti dati personali è necessario comunicare al Titolare o l'area ftp su cui dovrà caricare i file oppure per i Titolari con l'ambiente installato sul ns. data center, richiedere l'autorizzazione per far effettuare la copia ai nostri sistemisti.

Area FTP

L'area ftp sarà impostata affinché il Titolare veda solo l'upload. Il download sarà visualizzato solo dal gruppo di assistenza a cui la richiesta di assistenza è stata effettuata.
Tre giorni dopo la data di pubblicazione una routine cancellerà i file caricati in area ftp.

Area SharePoint

Essendo diventato Office 365 strumento aziendale anche di collaborazione ogni utente Zucchetti ha a disposizione Sharepoint che può utilizzare anche tale strumento per la condivisione dei documenti e file in genere coi clienti.

L'azienda al fine di tutelare la privacy del dipendente non entrerà nel merito dello sharepoint individuale, pertanto, una volta che il cliente ha scaricato i files, l'operatore avrà anche la responsabilità della relativa cancellazione.

Scaricamento archivi tramite wetransfer o link di collegamento su ambienti del Titolare
In questo caso la gestione è in carico al Titolare che fornirà le credenziali per accedere all'ambiente dove risiedono gli archivi.

L'assistenza dovrà scaricarli in dischi di rete non soggetti a backup e cancellarli al termine dell'attività come nelle altre ipotesi.

Autorizzazione di backup da parte dei nostri sistemisti
L'archivio ricevuto viene scaricato su una directory del gruppo di assistenza non soggetta a backup.
L'assistenza di primo livello trasmette il db all'assistenza di 2 livello. L'assistenza di 2 livello procederà alle analisi di cui il problema necessita e poi cancellerà gli archivi ricevuti.
In ogni caso l'assistenza che ha in carico il problema, sia essa di primo o secondo livello, al termine dell'attività, cancellerà gli archivi ricevuti.
L'assistenza che ha in carico la gestione, terminata l'attività dovrà cancellare gli archivi ricevuti dal disco condiviso e da eventuali supporti di memorizzazione locali.
Qualora vi fosse la necessità di mantenere gli archivi sarà mandata una email al Titolare che ne darà l'autorizzazione.
Gli archivi dei Titolari non potranno mai essere trasmessi a gruppi di lavoro differenti rispetto a quelli finalizzati alla risoluzione del problema segnalato dal Titolare.
L'unica possibilità che i tecnici hanno per conservare gli archivi senza la previa autorizzazione del Titolare è l'anonimizzazione degli stessi.

Assistenza attraverso la necessità di avere il backup dei clienti di un servizio data center
Qualora i dati personali del Titolare siano su sistema Zucchetti/Data center, in nessun caso l'assistenza di 1 livello potrà richiedere il backup ai sistemisti di Data center se non previa autorizzazione del Titolare stesso.
I sistemisti non potranno estrarre nessun backup dei Titolari per esigenze e finalità differenti rispetto al fornire assistenza agli stessi; ad esempio, non potranno essere effettuati backup indirizzati alla produzione per l'esecuzione di test.

Assistenza attraverso collegamento da remoto Team Viewer
Questa modalità di collegamento sugli strumenti dei Titolari garantisce la privacy in quanto:

- Il collegamento è sempre richiesto dal Titolare;
- le credenziali di accesso sono sempre individuali;
- il Titolare fa accedere i tecnici Zucchetti ad un ambiente con profilo di autorizzazione da lui scelto per far eseguire le attività di assistenza;
- il Titolare può disconnettere il tecnico quando desidera.

Attraverso Team Viewer è possibile far accedere anche l'assistenza di secondo livello alla stessa sessione aperta. In questo caso il Titolare ne ha l'evidenza perché fornita dallo strumento e quindi accetta implicitamente tale modalità
È essenziale utilizzare il Team Viewer Zucchetti in quanto licenziato e personalizzato con tutta la documentazione che deve essere prodotta dalla legge sul trattamento dei dati personali.
Solo in casi eccezionali e dopo attenta valutazione del responsabile e dell'ufficio privacy è possibile utilizzare altri strumenti di connessione che si comportano in modo uguale.

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.

Regole che riguardano gli ambienti dei Titolari, in qualsiasi forma di delivery (Saas/Paas/On Premise) riferite a:

- creazione utenze per consulenti applicativi;
- creazione utenze per personale di assistenza.

Consulenti applicativi

Per effettuare tutte le attività di start up sull'ambiente del Titolare è necessario che venga appositamente creata un'utenza all'interno del sistema come di seguito indicato:

- ZU_+ prime 3 lettere del cognome + prime 3 lettere del nome;
- nella descrizione (nome completo) apporre: Utente Zucchetti.

In questo modo il Cliente potrà riconoscere la provenienza dell'utenza stessa.
Es: per il soggetto Rossi Mario dovrà essere creata l'utenza: ZU_ROSMAR.

Per la creazione dovrà essere coinvolto il Titolare, il quale dovrà essere guidato all'accesso e alla creazione dell'utenza precisando e condividendo con lui, i diritti che verranno assegnati a quest'ultima.

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.
Anche in questo caso, per la creazione delle utenze, valgono le regole di creazione esplicitate per i consulenti applicativi

Le utenze dovranno essere generate con la codifica: ZU_prime tre cognome_prime tre nome.
Nella descrizione dovrà essere inserito Zucchetti Utente

Conversioni e progetti di start up

Qualora si verifichino le seguenti casistiche:

- Conversione o start up con contratto
- Conversioni o startup senza contratto

Nel primo caso le attività sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite.
In questo caso è necessario redigere un documento di progetto in cui si convengono con il Titolare le modalità operative di esecuzione delle attività tra cui:

- Dati personali, archivi, base dati di cui necessita l'esecuzione delle attività;
- dettaglio delle operazioni da eseguire sui dati;
- identificazione del periodo entro cui sarà terminata tale attività;
- la previsione di un collaudo in cui il Titolare proverà la conversione.

I documenti che il Titolare ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Zucchetti di svolgere tutte le attività necessarie all'erogazione del servizio.
In questo caso non serve mandare al Titolare la lettera di incarico, in quanto la stessa viene fatta da Zucchetti, in qualità di responsabile, agli addetti Zucchetti.

Qualora non vi sia il contratto invece è necessario inviare al Titolare la nomina a responsabile al trattamento.
Nella nomina dovrà essere previsto un termine di svolgimento e portata a termine dell'attività. Zucchetti provvederà ad incaricare gli addetti in qualità di responsabile.
Anche in questo caso è necessario prevedere una fase progettuale in cui condividere gli step sopra riportati.
Al termine sarà anche in questo caso essenziale prevedere il collaudo.

Con il documento di collaudo, che dovrà essere sottoscritto dal Titolare, lo stesso ci dichiarerà che le attività da noi effettuate sono corrette e quindi ci autorizzerà a cancellare i suoi archivi.
Nel documento di collaudo dovranno essere inserite le seguenti indicazioni:

- Il lavoro svolto è conforme rispetto all'ambito contrattuale convenuto;
- il Titolare ha provato la conversione e dichiara che il prodotto funziona e tutte le funzioni sono state correttamente configurate e implementate;
- che non ci sono errori nei dati convertiti e che quindi potrà utilizzare il prodotto per le finalità per cui lo ha acquistato.

Inoltre, il Titolare deve dichiarare che dalla data della firma del contratto non avrà nulla a pretendere rispetto all'attività di conversione svolta e prevista dal contratto e che autorizza Zucchetti a cancellare ogni dato, archivio, data base che è servito per portare a termine la fase di conversione.
Solo qualora ci fosse la necessità di mantenere gli archivi del Titolare per finalità di cautela e verifica del lavoro da noi svolto, dobbiamo inviare una comunicazione con la quale il Titolare ci autorizza a conservare gli archivi per l'ulteriore periodo, terminato il quale gli archivi dovranno essere eliminati.
Tutto l'iter autorizzativo dovrà essere inserito nel post-vendita al fine di averne memoria.
Tutti i documenti contenenti dati dei Titolari stampati non possono essere riutilizzati come carta da riciclo e devono essere immediatamente distrutti.

Categorie di destinatari a cui i dati potrebbero essere comunicati

Non è prevista, da parte del Responsabile del trattamento, la comunicazione dei dati a soggetti terzi.
Il Titolare deve attivare l'utenza al medico amministratore, il quale a sua volta può abilitare le utenze degli eventuali altri medici competenti e le utenze del personale paramedico.

Periodo di conservazione dei dati personali

Non sono previste procedure automatiche di cancellazione, ma la stessa deve avvenire in modo dedicato e specifico su ogni soggetto da parte del Cliente.
I dati conservati nel Data Center Zucchetti saranno conservati per tutta la durata del contratto e per i 90 giorni successivi alla sua cessazione. Saranno conservati su supporti di backup per i successivi 12 mesi.
I dati trasmessi attraverso lo strumento di ticketing, per finalità di assistenza, vengono conservati nello strumento stesso per 5 anni dalla chiusura del ticket.

Finalità del trattamento cui sono destinati i dati personali

La finalità dell'applicativo è quella di mettere a disposizione dei medici competenti uno strumento che consenta di gestire, in forma informatizzata, l'idoneità alla mansione, la cartella sanitaria e di rischio del lavoratore, come previsto dall'art 25 comma 1 lett c. del D.Lgs. 81/2008. Il modulo consente altresì di allegare l'esito delle visite mediche.

Ambito di conoscenza dei Suoi dati

I dati trattati dell'app sono trasmessi al prodotto software HR Portal. I dati saranno visualizzabili dal Datore di lavoro in funzione dei profili autorizzativi dallo stesso assegnati nell'ambito della sua organizzazione sugli applicativi sopra citati. Il fornitore del servizio non è autorizzato a visualizzare i dati personali registrati bensì solo ad eseguire attività di manutenzione applicativa e sistemistica sul servizio offerto. Qualora vi sia la necessitò di accedere ai suoi dati personali il fornitore richiederà preventivamente l'autorizzazione al cliente/Titolare del trattamento che la dovrà informare prontamente della necessità e sulle misure di sicurezza adottate a tutela dei suoi dati.

Ambito territoriale del trattamento

I dati forniti saranno trattati in Italia.

Diritti degli interessati

Potrà esercitare i Suoi diritti inviando una e-mail a ufficio.privacy@zucchetti.it, in particolare potrà richiedere l'accesso ai dati personali che la riguardano, la rettifica o la cancellazione o potrà richiedere la limitazione al trattamento e potrà opporsi al trattamento. Inoltre, avrà il diritto alla portabilità dei dati e qualora volesse proporre reclamo potrà presentarlo anche all'autorità Garante per la protezione dei dati personali.

Privacy rules applying to Zucchetti APPs

pursuant to Article 13 of the European General Data Protection Regulation 2016/679 (GDPR)

This Privacy Policy is provided exclusively for the Zucchetti **ZSafe PRO MED** application but not for any websites through which, for example, the User might access or use the application.

Data Controller

The data controller, pursuant to Article 4, point 7 of the GDPR, is Zucchetti S.p.A., with registered office in Lodi, Via Solferino no. 1, 26900 – e-mail: ufficio.privacy@zucchetti.it.

Data Protection Officer

The data protection officer is Mr. Mario Brocca, who may be contacted by writing an email to mailto:dpo@zucchetti.it.

Developer

The Developer of the application is InfoFactory S.r.l., with registered office in Via Jacopo Linussio 51, Udine 33100- Contact person Massimiliano Valotto valotto@infofactory.it

Personal data collected

The services provided by the App, as well as the features and functions of the same, do not require any form of User registration. However, we would like to point out that, during their normal operation, the IT systems and software procedures used to operate the App (such as Apple Store or Google Play), acquire certain data referring to the User whose transmission is implicit in the use of the Internet communication protocols, smartphones and devices used. This data category includes, without limitation, the geographical position, phone ID, User contacts, e-mail address and credit card details.
The User can consult the Privacy information available on the following websites:

- Apple Store- http://www.apple.com/legal/privacy/it/
- Google Play- https://www.google.it/intl/it/policies/privacy/

The **ZSafe PRO MED** app collects the following personal data:

- **Camera**: to read a combination of data within a QR code to configure the app, to automatically pre-fill the data during compilation and to obtain an image of any documents to be recorded in the worker's health and risk folder. Images are saved to a memory location on the phone that is not accessible to the user outside the app. Images captured as attachments are sent to the server that stores them in the Document Management System. They can be deleted at any time by the customer;
- **Microphone:** possibly used only by the device's virtual keyboard. No data is saved in the app;
- **Biometric data**: biometrics are managed directly by the manufacturer of the device inside the device itself. Zucchetti, as the application producer, does not know where or how the biometric data are stored on the device and cannot access them. The only activity carried out by Zucchetti is to query the operating system to request the validation of biometric credentials, which may or may not be confirmed by the OS, without any visibility into the process and the underlying biometric data;
- **Username, password and connection URL** necessary to access the functionalities of the app.

It also collects and manages the following personal data:

- **Worker's personal data** (surname and first name, gender, place of birth, date of birth, address, nationality, tax code, job classification);
- **data relating to the employment contract** and contract job description, role, documentation necessary for the management of employment relations (e.g. identity cards, training);
- **data relating to the health status of the worker** and/or their family members (preventive medicine appointment, work history, family history, medical history, history of past illnesses, history of current illnesses, physical examination [with particular reference to the target organs], additional investigations, any measures taken by the occupational physician, fitness to work on the specific task or tasks).

Mandatory or optional nature of data provision and consequences of any refusal

The provision of data is optional but necessary to provide the service. Refusal to provide the same will not allow provision of the service or use of the app.

Processing methods

Data are processed in electronic format and, when the app is in use, the workers' personal data is re-routed through secure connections to the HR Portal web software product produced by Zucchetti. The above data are never permanently saved on the device. The user (physician) can delete the data at any time using the functions present in the app.

Secure procedures for processing personal and sensitive user data

The developer has developed and implemented secure data processing procedures consisting of security measures at the technical and organisational level, as well as at the level of assistance services.
In particular, the security measures that can be configured at the application level are:

- Management of access credentials
  - Username: access to the App is subject to the Data Controller authorising its employees/collaborators, who can download the App independently. Access is granted only through the unambiguous identification of the person that accesses the app. There are administrative credentials in the system that are provided to the Data Controller and that can be used by the above only in exceptional circumstances. The Data Controller must put in place an organisational procedure so that this username is assigned to a single officer and managed in compliance with good management practices. A Customer/Owner user is profiled in the system as a Medical Administrator. The Data Controller must put in place an organisational procedure so that this username is assigned to a single officer and managed in compliance with good management practices. In particular, the system administrator must enable the Medical Administrator's access (the system administrator is a user belonging to group 1-Zucchetti Administration). The system administrator enters the identification data of the doctor, who receives a notification informing them that they have been designated "Medical Administrator" for the purpose of managing the health records of workers and that, to confirm this designation, it is necessary to connect to the Portal and enter the assigned identification data. If the information entered by the Medical Administrator matches the data entered by the System Administrator, the physician's authorisation is confirmed and the latter can proceed to activate the OTP for their user profile. Once the Medical administrator's account has been enabled, the user can register their device via the mobile app;
  - password: the password complexity rules are configurable in the system by the Data Controller. The same may choose different degrees of complexity and apply them to all system users. Password replacement times are also configurable;
  - complexity criteria for setting credentials
    - access credentials can be set according to different complexity criteria by the Data Controller;
    - the Customer has the option of uploading into the Blacklist Password a dictionary of passwords, which does not allow users to enter non-complex passwords;
    - the Customer can set the timed account blocking function or account blocking for exceeding the number of failed login attempts. There is also the possibility to set a maximum number of login attempts and a maximum number of password changes in one day.
  - credential deactivation/disabling: the deactivation times of unused credentials or the disabling of the credentials of employees who no longer have the personal characteristics to access such personal data can also be configured in the system by the Data Controller;
  - to use the app, a two factor authentication through an OTP system is required.

- Minimisation
  - Authorisation profiles: the Data Controller can configure access to personal data processed in the system according to the activities carried out by users. In detail, the following authorisation profiles can be configured:
    - Medical administrator, who has access to all sections of the system, can read and edit them and has the right to enable doctors to access health data;
    - Company doctor/healthcare operator, who has (reading and editing) access to the sections of the health data according to the authorisation profile configured by the Medical administrator.

- Identification of the people who processed the data
  - Log tools: the Data Controller can activate the logs of the procedure used to register accesses to the procedure itself through the functions of the HR Portal. The log must be extracted by the Data Controller and is stored in the system for 45 days, extendable to up to 365 days during configuration;
  - The various operations carried out (viewing, editing, deletion of data, printing, attribution of authorisation profiles by the medical administrator) are tracked on the health record; the system records an encrypted log containing the user code, surname and name of the person who carries out the validation and the date and time in which validation is completed. Logs are not deleted;
  - Presence of service usernames for support personnel: the people who perform support and maintenance on the procedure have usernames associated with them that must be activated and deactivated by the Data Controller according to need.

- Encryption techniques
  - Password encryption: a password hash is registered with the bcrypt algorithm, adding an application "salt" and a user "salt";
  - crypting password DB service account;
  - encryption of application tables: the data relating to the worker's medical history and physical examination are written in independent and encrypted tables; the tables containing health data are encrypted and do not contain direct references to the worker to whom they refer; application access is always guaranteed through encryption;
  - on the mobile device, all data used in mobile mode are encrypted in a local database. Each user registered on the app of a single device has their own encrypted local database. The data to access the database and the web server are encrypted in the SecureStorage of the device;
  - the data exchange between the app and the web server is encrypted in application layers with symmetric and asymmetric encryption techniques, regardless of any transport-level encryption (HTTPS);
  - database encryption: it is possible to encrypt the database using the standard tools made available by the various DB-Engines, such as TDE (Transparent Data Encryption), limited to Saas and Paas services and on facilities from 2006. The option can only be activated at the design level on hosting;
  - encryption of DMS files: all documents generated by the applications and stored in the DMS are encrypted; the encryption for any documents generated externally and stored in the DMS will be applied by correctly setting the parameters on the "Document Class" associated with the documents themselves.

- Privacy by default
  - User profile activation: users are activated in the portal according to a logic of not assigning any authorisation profile on the processed data. It is up to the Data Controller, at their discretion, to choose the appropriate user profiling and assign authorisations according to the homogeneous area to which the user or the individual authorisation profile belongs.

- Rights of Data Subjects
  - Rights of the Data Subject: in order to guarantee data subjects the right to anonymity, it is sufficient that they send a request to the Data Controller which will perform the appropriate assessments. Should the Data Controller decide that the data must be deleted, the same may act directly on the HR Portal, thus deleting the personal data in each HR area application; no information, not even indirect, will be subsequently retrievable with regard to that data subject. Therefore, in individual applications there will only be anonymous information not referable, not even indirectly, to any data subject. The deletion functions are executed by subject registration data;
  - to guarantee the right of the data subject to have information on which data the Data Controller processes and on the portability of the subject's data, there is the possibility in the HR Portal to make HTML extractions of both the personal details part as well as all application parts concerning that data subject. With the HTML, the Data Controller can transmit the data to the data subject, who will be able to process it for his/her own purposes. Should the HTML not be sufficient, the export can take place in XML or CSV format;
  - the Customer can anonymise the personal data of data subjects with specific queries. This function concerns the tables but not note fields; no checks can be activated on note field contents at the procedure level.

The system is set up with the pseudo-anonymisation of personal data in terms of the personal information of data subjects. Only customers that have chosen to manage links by tax code cannot use this security technique.

With regard to support procedures, **processing security** is ensured for each type of support in the following ways.

On Site Support

Zucchetti employees access the Data Controller's facility for training or carrying out technical maintenance activities.
In this case, Zucchetti employees work as if they were part of the Data Controller's structure and adopt all the security procedures implemented by the same. Data Controllers will be able to generate individual usernames for access to their systems or may allow access alongside personnel for their training.
Should the Zucchetti employee need to retrieve archives or DBs during the support activity to solve any problems, it is necessary that he/she informs the Data Controller and records this activity in the Service Note:
At the end of the activity at the Zucchetti offices, the Data Controller will be informed about the solution adopted and subsequent deletion of the archive.
Should it be necessary to retain the archives for the time required to test the solution adopted, the Data Controller must be informed about the maximum storage time of these archives.

Telephone Support

This does not have any problems from a personal data processing point of view. No data or archives are transmitted and communication is verbal only.

Support Via Email/Web Tickets

In the case of support by email, the Zucchetti technicians will always include the disclaimer in the message text to inform the Data Controller of the summary policy and of the persons to contact in order to exercise its rights or the rights of its data subjects.
The Zucchetti employee is not authorised to have the Data Controller's access credentials sent by email nor may he/she save them on the ticketing tool.
If the Data Controller sends the access credentials to its environment without the Zucchetti technician's request, it is necessary that the technician replies that they are not authorised to access the systems with the credentials of other users since this violates the GDPR. The Zucchetti technician must thus request individual credentials or a remote connection through dedicated tools.
The Zucchetti technicians will sign each email with name and surname and the information will be saved in the ticketing tool.

Support by receiving Customer Databases

Should it be necessary to have the database or other files or queries containing personal data sent in order to solve the problem reported by the Data Controller, it is necessary to communicate to the Data Controller either the FTP area in which to upload the files or, for Data Controllers with the environment installed in our data centre, request authorisation to have our system engineers make a copy.

FTP Area

The FTP area will be set so that the Data Controller sees only the upload. The download will only be viewed by the support group to which the support request was made.
Three days after the publication date, a routine will delete the files uploaded to the FTP area.

SharePoint Area

Since Office 365 has also become a corporate collaboration tool, every Zucchetti user can use Sharepoint also to share documents and files in general with customers.
In order to protect the employee's privacy, the company will not enter into the merits of the individual Sharepoint; therefore, once the customer has downloaded the files, the operator will also be responsible for their deletion.

Download of archives via WeTransfer or links to Data Controller's environments

In this case, management is the responsibility of the Data Controller which will provide the credentials to access the environment where the archives reside.
Support must download them on network disks not subject to backup and delete them at the end of the activity as well as in other cases.

Authorisation to make a backup by our systems engineers

The received archive is downloaded in a directory of the support group that is not subject to backup.
First level support transmits the DB to 2nd level support. 2nd level support proceeds with the analyses that the problem requires and will then delete the received archives.
In any case, the support group that has taken charge of the problem, be it first or second level, will, at the end of the activity, delete the received archives.
The support group that is dealing with the problem, once the activity has been completed, must delete the archives received from the shared disk and any local storage media.
Should it be necessary to retain the archives, an email will be sent to the Data Controller which will provide the authorisation.
Data Controller archives can never be transmitted to work groups other than those engaged in solving the problem reported by the Data Controller.
The only way in which technicians can retain the archives without the prior authorisation of the Data Controller is via their anonymisation.

Support through the need to have a backup of customers of a data center service

If the personal data of the Data Controller are on a Zucchetti/Data Centre system, under no circumstances may 1st level support request a backup to the Data Centre system engineers without the prior authorisation of the Data Controller.
The system engineers may not extract any backups of Data Controllers for needs and purposes other than providing support to the same; for example, backups for production to be used for testing may not be made.

Support through remote Team Viewer connection

This method of connection on Data Controller tools ensures privacy since:

- The connection is always requested by the Data Controller;
- The access credentials are always individual;
- The Data Controller lets Zucchetti technicians access an environment with the authorisation profile chosen by the Data Controller in order to carry out the support activities;
- The Data Controller can disconnect the technician when they wish.

Through Team Viewer it is also possible to provide access to 2nd level support in the same opened session. In this case, the Data Controller has evidence of this since it is provided by the tool and, therefore, they implicitly accept this mode.
It is essential to use the Zucchetti Team Viewer since it is licensed and customised with all the documentation that must be produced by the law on the processing of personal data.
Only in exceptional cases, and after careful assessment by the manager and the privacy department, can other connection tools be used that behave in the same way.

Support through remote connection on public IPS or via VPN

If the support activity is to be carried out on cloud systems on public IPs or via VPN or private accesses, Zucchetti employees must enter Data Controller systems:

- Subject to authorisation of the customer;
- Subject to receiving individual credentials, which have been activated for the time necessary to perform the requested activities;
- the credentials are deactivated by the Data Controller at the end of the activity.

Rules concerning Data Controller environments, in any form of delivery (SaaS/PaaS/On Premises) referring to:

- creation of users for application consultants;
- creation of users for support personnel.

Application consultants

To perform all the start-up activities on the Data Controller environment, it is necessary that a username is specifically created in the system as follows:

- ZU_+ first 3 letters of the surname + first 3 letters of the name
- in the description (full name) enter: Zucchetti User

In this way the customer can recognise the origin of such username.
E.g.: for Rossi Mario, the following username must be created: ZU_ROSMAR.

The Data Controller must be involved in the creation and be guided in access and creation of the username, specifying and sharing with the same the rights that will be assigned to the username profile.

Help Desk personnel

The request for creation of the username must made only to the Data Controller which, through the application administrator, can create the new username.
The administrator user account must never be used by the support operators.
The creation rules set out for application consultants also apply to the creation of user accounts.

User accounts must be generated with the encoding: ZU_surname first three letters_name first three letters.
Zucchetti User must be entered in the description.

Conversions and start-up projects

In the following cases:

- Conversions or start-up with a contract
- Conversions or start-ups without a contract

In the first case, the activities are aimed at fulfilling the contractual obligation and are therefore legal.
In this case, it is necessary to draw up a project document in which the operating procedures for carrying out the activities are agreed with the Data Controller, including:

- Personal data, files, databases that execution of the activities requires;
- Details of the operations to be performed on the data;
- Identification of the period within which this activity will be terminated;
- The inclusion of an acceptance test in which the Data Controller will test the conversion.

The documents that the Data Controller has signed for the performance of these activities constitute the contract and appointment as data processor, conferring a mandate to Zucchetti to perform all the activities necessary for provision of the service.
In this case, it is not necessary to send the Data Controller the letter of appointment, since this is done by Zucchetti, as data processor, to the Zucchetti employees.
If there is no contract, it is necessary to send the Data Controller the appointment as data processor.
The appointment must include a deadline for carrying out and completing the activity. Zucchetti will appoint the employees as data processors.
Also in this case it is necessary to envisage a design phase in which the above steps are agreed.
At the end, also in this case, it will be essential to envisage acceptance testing.
With the acceptance test document, which must be signed by the Data Controller, the same will declare that the activities carried out by us are correct and therefore authorise us to delete their archives.

The following must be included in the acceptance test document:

- The work performed is compliant with the agreed contractual framework;
- The Data Controller has tested the conversion and declares that it works and all the functions have been correctly configured and implemented;
- That there are no errors in the converted data and that it can therefore use the product for the purposes for which it was purchased.

In addition, the Data Controller must declare that from the date of signing the contract, it will have nothing to claim with regard to the conversion activity carried out provided for by the contract and authorises Zucchetti to delete any data, archive or database used to complete the conversion phase.

Only if it is necessary to retain the Data Controller's archives for the purpose of precaution and verification of the work carried out by us, must we send a communication in which the Data Controller authorises us to retain the archives for a further period, after which the archives must be deleted.

The entire authorisation process must be entered in after-sales in order to have a record of it.
All documents containing printed Data Controller data may not be re-used as recycled paper and must be immediately destroyed.

Categories of recipients to whom the data may be communicated

The Data Processor is not required to disclose the data to third parties.
The Data Controller must activate the user profile of the Medical administrator, who in turn can enable the user profiles of any other company doctors and the user profiles of paramedical staff.

Personal data retention period

There are no automatic deletion procedures, but the Customer must delete each subject's data in a dedicated and specific way.
The data stored in the Zucchetti Data Center will be retained for the duration of the contract and for 90 days following its termination. It will be stored on backup media for the next 12 months.
The data transmitted through the ticketing tool, for assistance purposes, are kept in the tool itself for 5 years from the closure of the ticket.

Purpose of personal data processing

The purpose of the application is to provide company doctors with a tool that allows them to manage, in computerised form, fit-for-work assessments, the health and risk record of the worker, as provided for by Article 25 paragraph 1, sec. c. of Leg. Dec. 81/2008. The form also allows users to attach the outcome of medical examinations.

Scope of knowledge of your data

The data processed by the app are transmitted to the HR Portal software product. The data will be viewable by the Employer according to the authorisation profiles assigned by the same in the context of its organisation on the applications mentioned above. The service provider is not authorised to view the personal data recorded but only to perform application and system maintenance on the service provided. If it is necessary to access your personal data, the provider will request prior authorisation from the customer/Data Controller, which must promptly inform you of the need and the security measures adopted to protect your data.

Territorial scope of processing

The data provided will be processed in Italy.

Rights of Data Subjects

You may exercise your rights by sending an email to ufficio.privacy@zucchetti.it; in particular, you may request access to personal data concerning you, their correction or cancellation or you may request limitation of processing and may object to processing. You will also have the right to data portability and, if you wish to make a complaint, you can also submit the complaint to the Data Protection Authority.