[English version below]

Norme sulla privacy relative alle APP Zucchetti

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 questa specifica applicazione mobile **ZAsset Booker** 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 e-mail a dpo@zucchetti.it.

Sviluppatore

Lo Sviluppatore dell'applicazione è Zucchetti Spa, con sede legale in Lodi, Via Solferino n. 1, 26900 - ufficio.privacy@zucchetti.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 e 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/

Questa applicazione mobile raccoglie i seguenti dati:

- **Dati personali:** username, password, URL, dati anagrafica e generici sulla persona.
- **Dati applicativi:** prenotazioni delle risorse aziendali (scrivanie, sale, parcheggi, ecc), timbrature rilevate per effettuare check-in e check-out tramite click manuale, QR Code, Tag NFC. Fotocamera per configurare l'applicazione e per leggere una combinazione di dati all'interno di un QR code nelle sezioni di check-in e check-out.
- **Fotocamera** per configurare l'applicazione e per leggere una combinazione di dati all'interno di un QR code nelle sezioni di check-in e check-out.
- **Microfono**: dato che le funzionalità che necessitavano di questi permessi non sono state più implementate. Per questo ad oggi per queste funzioni non sono raccolti dati.

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 sono reindirizzati attraverso connessioni sicure al prodotto software web HR Portal prodotto da Zucchetti. I dati sopra riportati non sono mai salvati in via definitiva sul dispositivo. L'utente 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.

Gestione credenziali di accesso

- User name: 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 sono 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.
- 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 Titolare ha la possibilità di caricare in Blacklist Password un dizionario di password che non permette agli utenti l'inserimento di password non complesse.
  Il Titolare 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.
- Il sistema è configurabile con un sistema SSO attraverso un token, active directory, ldap, SAML 2.0, injection header. Nel caso di SSO l'App autentica l'utente sulla base di un certificato rilasciato con apposita procedura dal server. Se così configurata l'App non supporta più il local multi-user ed un device ammette un solo user. Viene inoltre disabilitata la funzionalità di cambio password dall'App.
- C'è una funzione CAPTCHA Block User account enumeration.

Minimizzazione

- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti.
  - *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 e alle singole funzioni che la compongono con il tipo di operazione eseguita. In particolare, è possibile attivare i log di verifica e controllo di ogni tabella applicativa (tra cui attività di inserimento, modifica e cancellazione). È il Titolare che deve scegliere quali tabelle monitorare.
- Il log dovrà essere estratto dal titolare e viene conservato nel sistema per 45 giorni.
- 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 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:

- 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 o effettuare attività tecnica di manutenzione. In questo caso gli addetti Zucchetti lavorano come se facessero parte della struttura del Titolare e 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 Titolare 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 e-mail/tickets web

Nell'assistenza tramite e-mail 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 e-mail 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 LogMeIn- Rescue.
I tecnici Zucchetti firmeranno ogni e-mail con nome e cognome e l'informazione sarà salvata nel ticketing.

Assistenza attraverso la ricezione di database 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.

<u>Area FTP</u>

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 collaboration 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 e-mail 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.
Ogni utente ha inoltre, in alternativa, a disposizione un'area 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 dell'area individuale, pertanto, una volta che il cliente ha scaricato i files, l'operatore avrà anche la responsabilità della relativa cancellazione.

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 LogMeIn – Rescue

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 LogMeIn – Rescue è possibile far accedere anche l'assistenza di 2 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 LogMeIn- Rescue 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.

Categorie di destinatari a cui i dati potrebbero essere comunicati
I dati personali raccolti potranno essere comunicati alle aziende del gruppo Zucchetti ed ai relativi subappaltatori. Inoltre, al fine di eseguire tutte le attività di assistenza e manutenzione, i dati raccolti potranno essere forniti a incaricati dell'Area Piattaforma Base HR & Tools e di tutte le aree collegate ai prodotti utilizzati dal Titolare, finalizzate ad eseguire attività di assistenza e manutenzione.

Periodo di conservazione dei dati personali
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.
Il Titolare ha la possibilità, attraverso le funzioni applicative di lanciare cancellazioni massive dei dati personali salvati nel db oppure di impostare la scadenza di visualizzazione di documenti nel dms e poi l'ads potrà accedere e cancellare tutti i dati di un determinato periodo.

Finalità del trattamento cui sono destinati i dati personali
I suoi dati verranno trattati per le seguenti finalità e nel rispetto delle basi giuridiche come meglio precisate. In particolare, a finalità di ZAsset Booker è supportare le aziende per una gestione sicura ed efficiente degli spazi lavorativi e delle risorse aziendali, semplificando i processi di prenotazione, assegnazione e monitoraggio.
La finalità del trattamento di Zucchetti è quella di assistenza e manutenzione dell'App. Il download dell'app è volontario ed in ogni momento l'utente può disinstallarla o modificare i permessi e le autorizzazioni affinché non siano più registrati dati personali quali la geolocalizzazione, o cancellare i documenti prodotti quali le note spese.

Ambito di conoscenza dei Suoi dati
I dati trattati dell'app sono trasmessi al prodotto Infinity ZAsset Booker. 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.
Per garantire agli interessati (utenti app) 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.

Privacy Policy concerning Zucchetti APPs

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

This Privacy Policy is provided exclusively for this mobile 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 art. 4 paragraph 7 of the GDPR is Zucchetti S.p.A. with registered office in Lodi, Via Solferino, 1, 26900 – e-mail zprivacy.officer@zucchetti.com

Responsible for data protection

The data protection officer is Dr. Mario Brocca, whom you can contact by writing an email to dpo@zucchetti.it.

Developer

The developer of the application is Zucchetti Spa, with registered office in Lodi, Via Solferino No. 1, 26900 - ufficio.privacy@zucchetti.it.

Personal data collected

The services provided by the App, as well as its features and functions, do not require any form of User registration. However, we point out that the computer systems and software procedures used to operate the App (such as Apple Store or Google Play) acquire, during their normal operation, some data in any case referable to the User whose transmission is implicit. in the use of internet communication protocols, smartphones and devices used. This category of data includes, by way of example but not limited to, the geographical position, the identity of the telephone, the User's contacts, e-mails, credit card data. The User can consult the Privacy information available on the following sites:

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

This mobile application collects the following data:

- **Personal data:** username, password, URL, personal and general data on the person.
- **Application data:** company resource reservations (desk, meeting rooms, car parks, etc.), clocking in to perform check-in and check-out via manual click, QR Code, NFC Tag. Camera to configure the application and to read a combination of data within a QR code in the check-in and check-out sections.
- **Camera** to configure the application, to set your own image in the app and to read a combination of data in an QR code in the check-in and check-out sections.
- **Microphone**: given that the functionalities that needed these authorizations have no longer been implemented. For this reason, no data are currently collected for these functions.

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

Processing takes place in electronic format and during use of the app the personal data is re-routed through secure connections to the HR Portal web software product produced by Zucchetti. The above data is never permanently saved on the device. The user can delete it at any time using the functions present in the app.
The data will be processed in Italy.

Secured procedures for handling personal and sensitive user data

The developer has developed and implemented secure data processing procedures consisting of security measures at both the technical organizational level and the support services level.
Application security measures:

Access credential management

- Username: Access to the App occurs after the Owner has enabled its employees/collaborators, who will be able to download the App independently. Access occurs only through the unique identification of the person accessing it. In the system there is an administrative credential that is delivered to the Holder and usable by the Holder are in exceptional circumstances. The Holder must set up an organizational procedure so that this user is assigned to a single appointee and is managed in accordance with good management rules.
- Password: Password complexity rules are configurable in the system by the Owner. He/she can choose different degrees of complexity and apply them to all users in the system. Password replacement times are also configurable.
- Complexity criteria for credential settings: login credentials can be set according to different complexity criteria by the Data Controller. Data Controller has the option of loading a password dictionary into Blacklist Password that does not allow users to enter non-complex passwords.
- Disabling/disabling credentials: disabling of unused credentials or the disabling of credentials of appointees who no longer have the subjective characteristics to access that personal data are also configurable in the system by the Data Controller.
- System is configurable with an SSO system through a token, active directory, ldap, SAML 2.0, injection header. In the case of SSO, the App authenticates the user based on a certificate issued by special procedure from the server. If so configured, the App no longer supports local multi-user and a device admits only one user. The password change functionality from the App is also disabled.
- There is a CAPTCHA Block User account enumeration function.

Minimization

- Authorization profiles: the Data Controller can configure access to personal data processed in the system depending on the activities performed by users.

Identification of who processed the data

- Log tools: the Data Controller can activate procedure logs with which accesses to the procedure itself and its individual functions are recorded with the type of operation performed. In particular, it is possible to activate the verification and control logs of each application table (including insertion, modification and deletion activities). Data Controller must choose which tables to monitor. The log must be extracted by the Holder and is stored in the system for 45 days.
- Service utilities for support personnel: those who perform support and maintenance on the procedure have named utilities that must be activated and deactivated by the Data Controller as needed.

Encryption Techniques

- Password encryption: a password hash is recorded using the bcrypt algorithm by adding an application "salt" and a user "salt"
- Crypting DB service account passwords.
- Database encryption: it is possible to encrypt the database using standard tools made available by the various DBEngine, such as TDE (Transparent Data Encryption), limited to Saas and Paas services and on installations from 2006 onwards. The option can only be enabled at the design level on hosting.
- DMS File Encryption: all documents generated by applications and stored in the DMS are encrypted; encryption for any externally generated documents stored in the DMS will be applied by correctly setting the parameters on the "Document Class" associated with those documents.

Privacy by default

- User profile activation: users in the portal are activated according to a logic of not assigning any authorization profile on the processed data. It will be the Owner autonomously to choose the suitable user profiling and to assign authorizations according to the homogeneous area to which the user belongs or the individual authorization profile.

Data Subject's rights

- In order to guarantee the data subject's right to have information about what data the Data Controller processes and to the portability of his or her data, within the HR Portal there is the possibility to make HTML extractions of both the master data part and any application part concerning that data subject. With the HTML, the Data Controller will be able to transmit the data to the data subject who will be able to process it for his or her own purposes. If the HTML is not sufficient the export may be in XML or CSV.

- The Client can anonymize the personal data of data subjects with special queries. This function concerns ta-belle but not note fields on whose contents no control can be activated at the procedure level.
- The system is set up with pseudo-anonymization of personal data with respect to the data subjects' master data. Only clients who have chosen to manage links by tax code cannot make use of this protection technique.

Support procedures security are implemented for each one:

Onsite support
Zucchetti employees access the Owner's facility to perform training or technical maintenance activities.
In this case, Zucchetti employees work as if they were part of the Owner's facility and adopt all security procedures implemented by the Owner. Holders may generate individual users for access to their systems, or they may have side-by-side access to train their staff.
If, during the service activity, the Zucchetti employee needs to retrieve archives or db's that he/she needs to resolve the highlighted issues, it is necessary that he/she informs the Holders and records this activity on the Intervention Note:
Upon completion of the activity at the Zucchetti offices the Holder will be informed about the solution adopted and the subsequent deletion of the archive.
If there is a need to keep the archives for the time necessary for the testing of the adopted solution, the Holder must be informed about the maximum retention time of these archives.

Telephone support
It presents no problems from a personal data processing point of view. No data or archives are transmitted, and communication remains verbal.

Assistance via email/web tickets
In email assistance, Zucchetti technicians will always include in the text of the message the disclaimer to make the Holder aware of the summary information and the contact details he or she can contact to exercise his or her rights or the rights of his or her data subjects.
The Zucchetti employee is not authorized to have the Holder's login credentials emailed to him or her, nor will he or she be able to save them on the ticketing tool.
If a Holder sends login credentials to his or her environment without a request from the Zucchetti technician, it is necessary for the Zucchetti technician to respond that he or she is not authorized to access the systems with other users' credentials because this mode violates the GDPR. So, the Zucchetti technician will have to request individual credentials or connection via LogMeIn - Rescue.
Zucchetti technicians will sign each email with first and last name and the information will be saved in ticketing.

Assistance through receipt of customer data base (telecare tools)
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 center, request authorization 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
SharePoint has become an enterprise collaboration tools and Zucchetti users may use it to share files with customers.
Employees privacy is safe because Zucchetti technician must delete the file when customer has finished downloading.

Download of files 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 files 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.

Authorization to make a backup by our systems engineers

The file received 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 analyzes that the problem requires and will then delete the files received.
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 files received.
The support group that has taken charge of the problem, once the activity has been completed, must delete the files received from the shared disk and any local storage media.
Should there be the need to retain the files, an email will be sent to the Data Controller which will provide the authorization.
Data Controller files can never be transmitted to different work groups compared to those engaged in solving the problem reported by the Data Controller.
The only possibility that the technicians have to retain the files without the prior authorization of the Data Controller is their anonymization.

Assistance through the need to have clients back up a data center service.

If the Holder's personal data is on a Zucchetti/Data center system, under no circumstances will 1-level support be able to request backups from Data center systemists unless authorized by the Holder himself.
Systematists will not be able to extract any backups from Holders for needs and purposes other than providing support to Holders; for example, no backups directed to production for testing purposes may be made.

Assistance through remote connection LogMeIn - Rescue

This mode of connection on the Holders' tools ensures privacy in that:

- the connection is always requested by the Holder;
- the access credentials are always individual;
- the Holder gives Zucchetti technicians access to an environment with an authorization profile chosen by the Holder to have support activities performed;
- the Holder can disconnect the technician whenever he/she wishes.

Through LogMeIn - Rescue it is also possible to have 2-level assistance access the same open session. In this case the Holder has the evidence because it is provided by the tool and therefore implicitly accepts this mode.
It is essential to use the Zucchetti LogMeIn - Rescue as it is licensed and customized with all the documentation that must be produced by the law on the processing of personal data. Only in exceptional cases and after careful evaluation by the manager and the privacy office is it possible to use other connection tools that behave in the same way.

Assistance through remote connection on public IP or via VPN

If the assistance activity is to be carried out on cloud systems over public IPs or via VPN or private access, it is necessary for Zucchetti employees to enter the systems of the Holders:

- upon customer authorization
- upon receipt of individual credentials and the credentials have been activated for the time necessary to perform the required activities
- upon completion of the activity the credentials are deactivated by the Holder

Rules affecting Holders' environments, in any form of delivery (Saas/Paas/On Premise) referring to:

- user creation for application consultants.
- user creation for support staff.

Application Consultants

To perform all start-up activities on the Owner's environment, a user account must be specially created within the system as below:

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

In this way the Customer will be able to recognize the origin of the user itself.
E.g.: for the subject Rossi Mario the user: ZU_ROSMAR will have to be created.
For the creation will have to be involved the Owner, who will have to be guided to the access and creation of the user specifying and sharing with him, the rights that will be assigned to it.

Help Desk

The creation of the user should be requested only from the Holder who, through the application administrator, will be able to create the new user.
The administrator user should never be used by the help desk personnel.
Again, the creation rules made explicit for application consultants apply to the creation of utilities.
Users should be generated with the coding: ZU_first three surname_first three first name.
Zucchetti User must be entered in the description.

Recipients to whom the data may be disclosed

The personal data collected may be communicated to companies in the Zucchetti group and their subcontractors. In addition, to perform all support and maintenance activities, the collected data may be provided to persons in charge of the HR Base Platform & Tools Area and all areas related to the products used by the Owner, aimed at performing support and maintenance activities.

Personal data retention period

Personal data collected in relation to the methods described above, will be retained for the duration of the contract and for 90 days after its termination. They will be retained on backup media for the next 12 months.
The Owner has the option through application functions to launch massive deletions of personal data saved in the db or to set the expiration date of viewing documents in the dms and then the ads will be able to access and delete all data for a given period. The data transmitted through the ticketing tool, for service purposes, are stored in the tool itself for 5 years after the closure of the ticket.

Personal data processing purposes

Data will be processed for the following purposes and in accordance with the legal bases as better specified. In particular, the purpose of ZAsset Booker is to support companies for safe and efficient management of workspaces and company resources, simplifying the booking, assignment, and monitoring processes.
The purpose of Zucchetti's processing is to support and maintain the app. Downloading the app is voluntary and at any time the user can uninstall it or change permissions and authorizations so that personal data such as geolocation is no longer recorded, or delete documents produced such as expense reports.

Scope of knowledge of your data

For the pursuit of the above-mentioned purposes, your data may be disclosed and processed, exclusively in Italy, will be viewable by the Employer in accordance with the authorization profiles assigned by him/her within his/her organization on the aforementioned applications. The service provider is not authorized to view the recorded personal data but only to perform application and system maintenance activities on the offered service. Should there be a need to access your personal data, the provider will request authorization in advance from the customer/Processing Owner, who must promptly inform you of the need and about the security measures taken 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 zprivacy.officer@zucchetti.com; in particular, you may request access to personal data concerning you, its 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 it to the personal data protection Authority. App users can a request to the Controller who will make the appropriate assessments. If the Data Controller decides that the data should be deleted, he can act directly on the HR Portal, by deleting the master data within each application of the HR area, no more information even indirectly about that data subject will be available. Thus, only anonymous information will be present in the individual applications that cannot be traced even indirectly to any data subject. Deletion functions take place by subject master data.