Norme sulla Privacy relative alla APP SICE4U - REGGIO EMILIA
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 SICE4U REGGIO EMILIA 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 EDILI REGGIO EMILIA – CASSA Ente bilaterale di mutualità ed assistenza, Via del Chionso, 22/a- 42122 REGGIO EMILIA- Codice Fiscale: 80010170357- Telefono 0522-500411 – Fax 0522- 500443 mail. info@edili-cassa.re.it pec. Direzioneedilicassa_re@pec.it.

Responsabile della protezione dei dati

Il responsabile per la protezione dei dati è B&P SOLUTION SRL Via Montefiorino, 10/1, 42123 Reggio Emilia (RE) telefono 0522/506307 mail: info@bepsolution.it pec: bepfuturoimmobiliaresrl@pec.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 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:

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

L'app SICE4U REGGIO EMILIA raccoglie i seguenti dati personali:

• User name, password, URL di collegamento e device ID, entrambi necessari per accedere alle funzionalità dell'app;
• Dati anagrafici e dati contributivi e retributivi. In base dati sono presenti i seguenti dati che presentano rischi specifici, detti dati particolari: opinioni politiche, dati relativi alla salute, situazione economica, ubicazione, appartenenza sindacale, ecc...

Natura obbligatoria o facoltativa del conferimento dei dati e conseguenze di un eventuale rifiuto
Il conferimento dei dati è necessario per l'erogazione del servizio. Il rifiuto al conferimento non consente l'utilizzo dell'app.

Modalità del trattamento

Il trattamento dei dati verrà effettuato mediante strumenti elettronici e/o telematici, e, in ogni caso, secondo le modalità e gli strumenti idonei a garantire la sicurezza e la riservatezza dei dati stessi, in conformità con quanto previsto dalla vigente normativa. In particolare, saranno adottate tutte le misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, come previsto dalla vigente normativa, in modo che sia garantito il livello minimo di protezione dei dati garantito dalla legge, consentendo l'accesso alle sole persone incaricate del trattamento da parte del Titolare o dei Responsabili designati dal Titolare.

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
• User name: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Il titolare
deve predisporre una procedura organizzativa affinché ogni utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione. Questa user name non potrà mai essere comunicata a chi non è stato formalmente incaricato a tale fine.
•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. Per l'applicazione Badge Cantiere l'impostazione periodo di validità della password è obbligatoria con un default previsto by design a 180 giorni di validità.
•Disattivazione/disabilitazione credenziali: anche i tempi di disattivazione delle credenziali inutilizzate o la disabilita- zione 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
•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.

- Gestione accessi:
L'accesso all'applicazione SICE4U REGGIO EMILIA, è subordinato alla creazione di credenziali da parte della Cassa Edile. Questa, in primo luogo dovrà generare credenziali univoche per ogni singolo utente. Post creazione, queste credenziali verranno inviate all'utente finale via e-mail, quindi verrà inviato lo username e una password temporanea, in aggiunta a questo, l'utente verrà settato come un "utente al primo accesso". L'utente, una volta ricevute le cre- denziali dovrà obbligatoriamente cambiare la password essendo temporanea.

- Tecniche di crittografia: Crittografia delle password: la password è concatenata a una stringa di caratteri noti, che è diversa per ciascun profilo utente, ed è "hashed" con l'algoritmo SHA-1. Questo è un algoritmo di hash crittografico unidirezionale. Il valore hash risultante è ciò che è memorizzato nel sistema. Quando è il momento di autenticare un profilo, il sistema utilizza la password di testo in chiaro immessa dall'utente (nella schermata di accesso, ad es.), Esegue lo stesso algoritmo e confronta il nuovo risultato crittografato con il risultato crittografato creato con la password usata.

- Tecniche di partizionamento:
Laddove possibile i dati identificativi personali sono separati dalle informazioni gestionali, a cui sono relazionati tra- mite id tecnici.
- Privacy by default
Attivazione profilo utente. 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 diretta- mente nelle singole applicazioni del Sistema Casse Edili anonimizzando l'anagrafica. In tal modo non sarà più reperi- bile alcuna informazione neppure indiretta sul soggetto interessato.
Il diritto dell'interessato ad avere informazione in merito a quali siano i dati trattati dal titolare e alla portabilità degli stessi, è garantito dalla presenza nell'applicazione di apposite funzioni ed estrazioni in formati standard. In tal modo il titolare potrà trasmettere i dati all'interessato che potrà trattarli per le sue finalità.
Il Cliente ha la possibilità di impostare la funzione di blocco account a seguito di un numero massimo di tentativi di immissione di una password scorretta.
Il collegamento al servizio in Cloud avviene tramite terminal server. Ad ogni licenza corrisponde un utente Windows che viene attivato, su richiesta del cliente, dal servizio sistemistico. Le credenziali inviate agli utenti sono da cambiare, nella componente riservata, al primo accesso all'ambiente.
NB: per quanto attiene al gestionale Ce.Net, allo stato attuale, non è ancora possibile configurare le regole di com- plessità della password e la funzione di blocco account, a seguito di un numero massimo di tentativi di immissione di una password scorretta.
Relativamente all'applicazione Badge Cantiere, la fase di richiesta ed approvazione del Badge tramite app dedicata è controllata dall'invio di un codice OTP di autenticazione della richiesta che verrà inviato dal sistema direttamente sul dispositivo del lavoratore che deve ottenere il Badge.

Queste misure di sicurezza devono essere correttamente impostate da parte del Titolare.
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 manu- tenzione.
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 database di cui neces- sita per risolvere le problematiche evidenziate è necessario che informi il Titolari e registri tale attività sulla Nota di inter- vento:
Al termine dell'attività presso gli uffici Zucchetti sarà informato il Titolari sulla soluzione adottata e sulla successiva can- cellazione 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 comu- nicazione rimane verbale.

- ASSISTENZA TRAMITE EMAIL/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 strumenti a ciò dedicati.
I tecnici Zucchetti firmeranno ogni e-mail 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 Share- point 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 riso- luzione del problema segnalato dal Titolare.
L'unica possibilità che i tecnici hanno per conservare gli archivi senza la previa autorizzazione del Titolare è l'anonimizza- zione 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 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 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 stru- menti 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 effet- tuate 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.
Periodo di conservazione dei dati personali
L'app SICE4U, riceve dati mediante l'utilizzo di servizi web, quindi non vi è alcun salvataggio di dati sensibili, se non il codice del lavoratore, il device ID e un determinato token di funzionamento per garantire la sicurezza nei vari accessi.
I dati personali raccolti in relazione alle modalità sopra descritte saranno conservati nell'app sino ad una sua cancellazione. Il Titolare ha la possibilità, attraverso le funzioni applicative di cancellare i dati personali salvati nel db.
Tutti questi dati, all'eliminazione dell'app vengo automaticamente rimossi dal dispositivo.
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.

I dati relativi alla gestione amministrativa e giuridica del rapporto contrattuale saranno conservati per 10 anni dalla cessazione del rapporto contrattuale.
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:
• Visualizzazione dati anagrafici presenti nei sistemi informatici della Cassa edile di appartenenza
• Visualizzazione liquidazioni/erogazioni ricevute dalla Cassa edile
• Ricezione di notifiche qualora fossero presenti nuove erogazioni
• Visualizzazione rapporti di lavoro in essere e/o conclusi
• Gestione dei documenti generati dai singoli applicativi
Ambito di conoscenza e diffusione dei Suoi dati
Per il perseguimento delle finalità sopra indicate, i dati potranno essere comunicati e trattati, esclusivamente in ambito nazionale, da soggetti terzi con i quali il Titolare intrattiene rapporti, come:
• soggetti autorizzati al trattamento da intendersi quali dipendenti o collaboratori del Titolare;
• responsabili del trattamento. Si precisa che il Fornitore del servizio non è autorizzato a visualizzare i dati personali
registrati, bensì solo ad eseguire attività di manutenzione applicativa e sistemistica in ragione del servizio offerto. Qualora vi sia la necessità 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. I dati potranno essere trattati anche da studio professionali genericamente intesi che possono fornire consulenza o assistenza di qualsivoglia genere al Titolare del trattamento.
• Token qui dentro forse, connessione con il gestionale, etc

Ambito territoriale del trattamento
I dati forniti saranno trattati in Italia.

Diritti degli interessati
Potrà esercitare i Suoi diritti inviando una e-mail a: info@edili-cassa.re.it - pec. Direzioneedilicassa_re@pec.it;
o scrivendo al Responsabile della Protezione dei dati B&P Solution, via e-mail. info@bepsolution.it - pec. bepfuturoimmobiliaresrl@pec.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 i diritti alla portabilità dei dati e qualora volesse proporre reclamo potrà presentarlo anche all'autorità Garante per la protezione dei dati personali.