Autore	Ufficio privacy Zucchetti S.p.a.
Approvazione	Marco Marchetti

Versione Revisione

Versione	Autore	Data	Motivo della revisione
0.0	Ufficio Privacy Zucchetti S.p.a.	07/12/2018	Prima emissione
1.0	Ufficio Privacy Zucchetti S.p.a.	25/09/2019	Inserito versioning; modificata la finalità del trattamento; specificati i termini di cancellazione dati per I servizi Cloud.
2.0	Ufficio Privacy Zucchetti S.p.a.	11/02/2020	Modifica del Fornitore del Servizio Cloud

PARERE DPO
OK.

OLTRE

RESPONSABILE DEL TRATTAMENTO					
Denominazione	ZUCCHETTI AXESS SPA				
Partita Iva	03537610960				
Indirizzo	VIA SOLFERINO 1				
Città	LODI	**Cap**	26900	**PV**	LO
Legale Rappresentante	DOMENICO UGGERI				

STRUTTURA ORGANIZZATIVA			
DIVISIONE	AXESS	**RESPONSABILE DIVISIONE**	MARCO MARCHETTI
AREA	OLTREMARE	**RESPONSABILE AREA**	ROBERTO FIDEL

INCARICATI DEL TRATTAMENTO
SVILUPPO COMMERCIALE POST VENDITA HELP DESK

DATI DI CONTATTO			
Titolare Del Trattamento	Zucchetti Axess S.p.a.	Ufficio.privacy@zucchetti.it	03715941
Rappresentante Del Titolare	N/A		
Responsabile Protezione Dati (DPO)	Mario Brocca	dpo@zucchetti.it	03715943191

DESCRIZIONE

La suite OLTRE è composta da un portale che gestisce servizi ai clienti attraverso diversi moduli integrati che gestiscono i seguenti processi: gestione delle presenze, turni, accessi, raccolta dati inizio e fine attività produttiva, raccolta dati da terminali fissi e mobili, gestione ronde.
ARUBA.php: è l'applicazione per la rilevazione presenze del personale aziendale che, anche con un'apposita app installata sul dispositivo mobile (OLTRE.app), consente al lavoratore di attivare il processo di presenza al lavoro. Con l'app è attivata anche la geolocalizzazione il cui controllo è in capo all'utente che può attivarla o disattivarla. È il cliente che ha acquistato i servizi a configurare il sistema in modo da avere o non avere il dato di geolocalizzazione nelle tabelle del database.
L'applicazione può anche gestire dati biometrici, qualora il cliente scelga di installare terminali biometrici. In questo caso la stringa alfanumerica corrispondente all'impronta digitale viene salvata in una tabella del database in modo che il dato possa essere distribuito a tutti i terminali.
ARBE.php: è l'applicazione che consente di gestire i turni di lavoro.
ELBA.php: è l'applicazione che gestisce il controllo degli accessi fisici, e consente di rilevare la geolocalizzazione dei terminali in modo da verificare la loro ubicazione spaziale. Anche in questo caso sono

salvate le coordinate di geolocalizzazione, ma riguardano la macchina e non le persone fisiche.
ANTIOPE.php: è l'applicazione utilizzata dall'azienda per la registrazione delle attività svolte sulle macchine di produzione (o a tavolino). Il lavoratore inserisce i tempi di inizio / sospensione / fine attività per evidenziare tutte le attività svolte e i tempi di lavorazione;
ANTIGUA.php: è l'applicazione che consente di scambiare dati con i terminali e i dispositivi mobili. Non sono trattati dati personali se ci si limita a raccogliere le transazioni senza associarle a una persona, se viceversa si gestisce un archivio delle persone con il relativo numero del badge, i dati personali vengono trattati (la scelta è opzionale al momento dell'ordine).
CATALINA.php: è l'applicazione che consente di gestire le ronde degli addetti alla sicurezza fisica e consente di evidenziare che siano stati visitati tutti i luoghi previsti dal contratto con il cliente.
Fanno parte del progetto anche altre applicazioni: per la gestione delle code e la prenotazione dei pasti.
PANAREA.php: è l'applicazione che consente di gestire, anche in modo anonimo, le code di attesa presso servizi pubblici e privati. Non sono trattati dati personali se ci si limita a ritirare un numero d'ordine di accesso alla cosa, se invece si gestiscono code che prevedono una prenotazione, i dati personali vengono trattati (la scelta è opzionale al momento dell'ordine).
PASTI.biz: è l'applicazione che consente la prenotazione dei pasti in ambiente ospedaliero, scolastico, aziendale. Le persone potranno scegliere il menu tra quelli disponibili, al fine di spedire le prenotazioni al fornitore per la preparazione dei pasti.

FINALITA' DEL TRATTAMENTO

La suite OLTRE è un sistema integrato che mette a disposizione applicativi software finalizzati alla semplificazione dei processi aziendali. Consente la registrazione delle presenze, degli accessi, dei turni di lavoro, dei tempi di svolgimento delle attività lavorative e di gestire l'infrastruttura hardware necessaria e propedeutica per le finalità descritte.
Alcuni applicativi, in particolari configurazioni, non gestiscono dati personali (ANTIGUA.php, PANAREA.php).
L'applicativo per la prenotazione dei pasti è stato realizzato con la logica di ottimizzare i tempi di preparazione dei pasti e di consentire la somministrazione del pasto in relazione alla dieta assegnata ed eventualmente alla preferenza.
Tutte queste funzionalità sono gestite da un unico sistema. Tutti i dati sono su base dati comune e quindi le sicurezze applicative sono comuni a tutti i servizi.
La finalità del trattamento è quella di erogare i servizi di assistenza e manutenzione al Titolare.

CATEGORIA INTERESSATI

La suite OLTRE è rivolta ad aziende: possono essere gestiti e trattati dati del personale dipendente, di collaboratori, visitatori e ospiti.

CATEGORIE DI DATI PERSONALI

Dati personali per lo più anagrafici. In funzione del servizio erogato i dati possono essere relativi alla presenza del personale, alle attività svolte dal personale e alla gestione dei turni di lavoro. In tutti questi casi sono trattati dati personali.
Dati che presentano rischi specifici: dati biometrici; coordinate di geolocalizzazione; dati relativi ai pasti/diete.

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

Solo per la versione Cloud i dati sono comunicati a AWS, gestore del Data Center e dei relativi servizi.

TRASFERIMENTO DATI FUORI DA UE

No.

TERMINI PER LA CANCELLAZIONE DEI DATI

Per i servizi Cloud, i dati vengono salvati in un file, il quale viene conservato per 40 giorni, mentre una volta che i dati sono trasferiti nel database sono automaticamente conservati per 3 anni e poi vengono cancellati; il cliente può comunque manualmente anticiparne la cancellazione.
Nella versione On-premises invece, in assenza di automatismi, la scelta della durata di conservazione del dato è lasciata al cliente.
Qualora un cliente risolva il contratto i dati sono conservati per i successivi 30 giorni e poi cancellati dall'ambiente di produzione. Sono conservati i dati di backup, al solo fine di conservazione, per i 12 mesi successivi.

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IN ESSERE

Le transazioni arrivano sul server tramite protocollo http o https, a seconda del terminale utilizzato dal cliente e della configurazione effettuata.
L'App OLTRE comunica di default tramite protocollo https, è possibile comunque configurarla in http (per la versione On Premise).

Quando viene attivato il servizio al cliente è consegnato un account di tipo 'superuser' con il quale può creare nuovi profili di autorizzazione. I profili di autorizzazione sono generabili sia per singola funzione che in relazione a quali eventi possono essere generati sui record del database (modifica, aggiunta, cancellazione, visualizzazione, stampa, elaborazione, ecc.). Non è possibile che ci siano più utenti con lo stesso nome.
Per ogni utente è possibile configurare le seguenti opzioni della password:

- Complessità (minuscole/maiuscole, numeri, caratteri speciali)
- Lunghezza (8-32 caratteri)
- Validità (da un giorno a 6 mesi)
- Numero di password precedenti non riutilizzabili
- Modifica obbligatoria o meno al primo login.

Le password sono crittografate nel database con SHA256
Le utenze vengono disabilitate automaticamente dopo 6 mesi di inattività.

C'è un log, sul database, di tutte le operazioni di modifica che sono operate nel sistema. I log sono conservati per 40 giorni (questo valore può essere configurato nelle versioni On-premises). I log sono visualizzabili per livello di autorizzazione.
È possibile cancellare i dati relativi a una persona, così come di esportarli in formato csv.
C'è la possibilità di cancellare i dati di un cliente con tutti i dati a lui collegati, così come di esportarli in formato csv.
È possibile archiviare in formato testo e/o cancellare i dati 'dinamici' (es.: transazioni di presenza, di accesso, dati del cartellino) di un singolo cliente. La funzione è disponibile anche per utenze non di tipo supervisore, purché abilitate.
I dati per principio di minimizzazione sono automaticamente conservati per 3 anni nella versione Cloud (durata non personalizzabile per cliente). Nella versione On-premises, priva di questo automatismo, sceglie il cliente, che ha la possibilità di storicizzare i dati e/o di eliminarli con funzioni applicative standard.
Tutto ciò che c'è nel database si può estrarre. Ogni estrazione e stampa può essere fatta con 'pdf creator'; i dati personali possono essere estratti in xml.

È prevista la possibilità di creare la crittografia per i dati relativi a:

- Coordinate di geolocalizzazione: il Titolare può limitare il numero di cifre decimali delle coordinate stesse, degradando così la precisione della posizione reale
- Per i terminali più recenti che lo consentono, è possibile abilitare la criptazione delle transazioni inviate.

2. MISURE DI SICUREZZA DA IMPLEMENTARE

Creare la crittografia per i dati relativi a:

- Dati biometrici: devono essere tutti crittografati soprattutto se è in uso il sistema per cui il dato biometrico risiede sull'HW e non sulla tessera dell'interessato
- Dati relativi alla dieta del paziente: verificare i campi tabella in cui poter implementare la crittografia in modo che i clienti che evidenziano la malattia a seguito del quale è fornita la dieta siano protetti da accessi non autorizzati a tali informazioni.
- Creare la crittografia per il passaggio/comunicazione dei dati tra sistemi: ad esempio per quanto riguarda le tabelle inviate;

Dare la possibilità anche ai clienti cloud di scegliere il tempo di conservazione dei dati. Oggi sono 3 anni per tutti, ma in funzione delle esigenze potrebbero avere richieste differenti.

3. MISURE DI SICUREZZA NELLE ATTIVITA' DI ASSISTENZA

Il servizio di assistenza ai prodotti e servizi della suite OLTRE è erogato verso:

- Clienti diretti
- Partner contrattualizzati come clienti
- Clienti cui l'assistenza è subappaltata ai partner

L'assistenza, in funzione della modalità di erogazione, viene effettuata in diversi modi.

Assistenza on-site

Gli addetti accedono presso la struttura del cliente per fare formazione o effettuare attività tecnica di manutenzione.

In questo caso lavorano come se facessero parte della struttura del cliente e adottano tutte le procedure che il cliente richiede di adottare. I clienti 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 si presentasse la necessità di prelevare archivi o database per risolvere le problematiche evidenziate è necessario informarne il cliente e scrivere nella Nota di intervento:

- L'archivio prelevato
- Le finalità per cui è stato prelevato l'archivio
- Il referente del cliente che ha autorizzato a prelevare l'archivio

Una volta risolto il problema segnalato va informato il cliente sulla soluzione adottata e sulla successiva cancellazione dell'archivio.

La email dovrà essere del seguente contenuto minimo:

"Stimatissimo Cliente Le comunico che il problema da Lei segnalato per la soluzione del quale c'è stata la necessità di prelevare i suoi archivi è stato risolto. Le comunico che abbiamo provveduto a eliminare gli archivi dai nostri sistemi informativi e a distruggere i documenti cartacei eventualmente prodotti."

Qualora vi fosse la necessità di conservare gli archivi per il tempo necessario al collaudo della soluzione adottata:

"Stimatissimo Cliente Le comunico che il problema da Lei segnalato per la soluzione del quale c'è stata la necessità di prelevare i suoi archivi è stato risolto. Le comunico che conserveremo gli archivi nei nostri

sistemi informativi per i prossimi 7 giorni. Al termine del periodo convenuto gli archivi saranno eliminati e non più ripristinabili".
Lo stesso iter dovrà essere seguito nel caso in cui si prelevasse l'archivio, si inviasse lo stesso al supporto e si risolvesse la problematica durante l'intervento c/o il cliente, senza necessità quindi di esaminarlo una volta tornati in sede.

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.
Bisogna prestare attenzione qualora il cliente informi che la telefonata viene registrata. Qualora vi sia l'avviso di registrazione bisogna annotare tale evento nel CRM in uso con l'indicazione dei riferimenti della struttura dei clienti a cui ci si può rivolgere per l'esercizio dei diritti di Zucchetti Axess.
Qualora fosse Zucchetti Axess a registrare le telefonate, il cliente andrà informato e bisognerà fornirgli le informazioni sui referenti a cui si potrà rivolgere per l'esercizio dei suoi diritti. Il riferimento per tale finalità dovrà essere ufficio.privacy@zucchetti.it. Anche in questo caso andrà annotato l'evento nel CRM.

Assistenza tramite email

Nell'assistenza tramite email va inserito sempre nel testo del messaggio il disclaimer:
"Il contenuto di questa email e degli eventuali allegati è strettamente confidenziale, non producibile in giudizio e destinato alla/e persona/e a cui è indirizzato. Il contenuto della risposta alla presente email potrebbe essere conosciuto anche da altri collaboratori facenti parte dello stesso Gruppo omogeno dello scrivente o di gruppi omogenei differenti ma speculari alla soluzione del problema da Lei segnalato. Se avete ricevuto per errore questa email, Vi preghiamo di segnalarcelo immediatamente e di cancellarla dal Vostro computer. E' fatto divieto di copiare e divulgare il contenuto di questa email. Ogni utilizzo abusivo delle informazioni qui contenute da parte di persone terze o comunque non indicate nella presente email, potrà essere perseguito ai sensi di legge. Si informa che per l'esercizio dei diritti previsti dagli artt. 15 e ss. del Regolamento UE 2016/679 (GDPR), è possibile rivolgersi al seguente indirizzo: ufficio.privacy@zucchetti.it".
Eventuali credenziali di accesso del cliente ricevute via email verranno rifiutate, non memorizzate e cancellate (quelle del cliente, non quelle generate appositamente per i tecnici che effettueranno l'assistenza, e che potranno essere anche ricevute via email): qualora un cliente/partner invii le credenziali di accesso al suo ambiente senza richiesta di Zucchetti Axess, gli verrà risposto che Zucchetti Axess non è autorizzata ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il Regolamento UE 2016/679 (GDPR). Quindi verranno richieste credenziali individuali oppure collegamento con strumenti di Desktop remoto (di uso commerciale).
Ogni email verrà firmata con il nome e cognome dell'operatore che ha gestito il problema del cliente e l'informazione sarà memorizzata nel CRM (è sufficiente anche il solo nome proprio, oppure il nickname Zucchetti Axess).

Assistenza attraverso la ricezione di data base dei clienti

Qualora per risolvere il problema segnalato dal cliente sia necessario farsi mandare la base dati o altri files contenenti dati personali, lo scaricamento archivi avviene tramite WeTransfer o link di collegamento su ambienti clienti: in questo caso la gestione è in carico al cliente che fornisce 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.

Assistenza attraverso la necessità di avere il backup dei clienti di un servizio Cloud

Nel CRM ci dovrà essere la prova dell'autorizzazione scritta o verbale del cliente.
I sistemisti non potranno estrarre nessun backup dei clienti per esigenze e finalità differenti rispetto al fornire assistenza ai clienti; ad esempio non potranno essere effettuati backup indirizzati alla produzione per l'esecuzione di test.

Assistenza attraverso collegamento da remoto

Questa modalità di collegamento sugli strumenti dei clienti garantisce la privacy in quanto:

- Il collegamento è sempre richiesto dal cliente
- Le credenziali di accesso sono sempre individuali
- Il cliente fa accedere a un ambiente con profilo di autorizzazione da lui scelto per far eseguire le attività di assistenza
- Il cliente può sconnettere il collegamento quando desidera

È essenziale utilizzare uno strumento licenziato per uso commerciale 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 entrino nei sistemi dei clienti:

- Previa autorizzazione del cliente
- Che abbiano le credenziali attive per il tempo necessario all'esecuzione delle attività richieste
- Che al termine dell'attività siano disattivate

Le regole che riguardano gli ambienti dei clienti, in qualsiasi forma di delivery (SaaS/PaaS/On-premises) sono le seguenti:

- Creazione utenze per consulenti applicativi:

Per effettuare tutte le attività di start up sull'ambiente cliente è necessario che venga appositamente creata un'utenza all'interno del sistema (che avrà il profilo utente 'Utente Zucchetti Axess') con questo 'login name': ZA_+ prime 3 lettere del cognome + prime 3 lettere del nome.
In questo modo il Cliente potrà riconoscere la provenienza dell'utenza stessa (es: per il soggetto Rossi Mario dovrà essere creata l'utenza: ZA_ROSMAR).
Per la creazione dovrà essere coinvolto il cliente, 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 (definizione del profilo utente).

- Creazione utenze per personale di assistenza:

Alla richiesta di assistenza verrà inviata un'email al cliente, che specificherà le informazioni necessaria alla creazione del 'login name' di chi effettuerà l'assistenza. Valgono le regole di creazione già esplicitate per i consulenti applicativi.
Al termine dell'assistenza verrà inviata un'email al cliente:
"L'attività di assistenza è terminata le ricordiamo di disattivare le credenziali al fine di tutelare i suoi dati personali".

Conversioni e progetti di start-up

Possono presentarsi due situazioni differenti:

- Conversione o start-up con contratto
- Conversione o start-up 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 cliente le modalità operative di esecuzione delle attività tra cui:

- Dati personali, archivi, base dati necessari per l'esecuzione delle attività
- Dettaglio delle operazioni che verranno eseguite sui dati
- Identificazione del periodo entro cui tale attività saranno terminate
- La previsione di un collaudo in cui il cliente proverà il buon esito del lavoro effettuato

I documenti che il cliente ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Zucchetti Axess di svolgere tutte le attività necessarie all'erogazione del servizio.
In questo caso non viene spedita al cliente la lettera di incarico, in quanto la stessa viene fatta da Zucchetti Axess, in qualità di responsabile, agli addetti Zucchetti Axess.
Qualora non vi sia il contratto invece è necessario inviare al cliente la nomina a responsabile al trattamento.
Nella nomina dovrà essere previsto un termine di svolgimento e portata a termine dell'attività. Zucchetti Axess 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 cliente, lo stesso dichiarerà che le attività effettuate sono corrette e quindi 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 cliente ha provato e dichiara che il prodotto funziona e tutte le funzioni sono state correttamente configurate e implementate
- Non ci sono errori nei dati convertiti e quindi potrà utilizzare il prodotto per le finalità per cui lo ha acquistato

Inoltre il cliente dovrà 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 Axess 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 cliente per finalità di cautela e verifica del lavoro svolto, andrà inviata una comunicazione al cliente che dovrà autorizzare Zucchetti Axess 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 in caso di necessità.
Tutti i documenti contenenti dati dei clienti stampati non possono essere riutilizzati come carta da riciclo e devono essere immediatamente distrutti.

4. MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI – CLOUD – EROGATI DA AMAZON WEB SERVICES

Le misure di sicurezza adottate dal fornitore del servizio cloud sono consultabili al seguente link: https://www.amazon.it/gp/help/customer/display.html?nodeId=201908990

Il fornitore è stato nominato responsabile del trattamento mediante apposito atto di nomina consultabile al seguente link: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Il Data Center è dotato di sistemi di protezione da intrusioni ostili (dispositivi di firewall e antivirus), che sono stati opportunamente configurati per garantire la sicurezza delle informazioni immesse e trattate dai clienti.