I SERVIZI E PRODOTTI ZUCCHETTI IN RELAZIONE ALLE PRESCRIZIONI DEL GDPR: INFINITY ZUCCHETTI

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Zucchetti Spa				
Partita Iva	05006900962				
Indirizzo	Via Solferino,1				
Città	Lodi	**Cap**	26900	**PV**	LO
Legale Rappresentante	Alessandro Zucchetti				

STRUTTURA ORGANIZZATIVA			
Divisione	Infinity Zucchetti	Responsabile Divisione	Giorgio Mini
Area	Soluzioni Infinity	Responsabile Reparto	Giovanna Mola

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

DATI DI CONTATTO			
Titolare del trattamento	Zucchetti Spa	Ufficio.privacy@zucchetti.it	03715941
Rappresentante del titolare			
Responsabile protezione dati (DPO)	Mario Brocca	Ufficio.privacy@zucchetti.it	03715943191

DESCRIZIONE

Infinity Zucchetti è la suite software completa per l'impresa che vuole gestire tutti i processi aziendali. Tutte le soluzioni della suite sono pensate e progettate per il web, quindi potenzialmente raggiungibili da qualunque luogo senza installazione locale (fruibili *on-cloud*).
La suite comprende le seguenti funzionalità: ERP (Ad Hoc Infinity, gestionale per medio/grandi aziende, composta dalle aree Amministrazione e finanza, Controllo di gestione, Ciclo Vendite, Ciclo Acquisti, Logistica), Fatturazione elettronica, CRM, E-commerce e portali aziendali, Gestione documentale, Collaboration & Communication, Business Intelligence & Analytics.

FINALITA' DEL TRATTAMENTO

Gestione dei dati personali di interessati che hanno rapporti con aziende ed enti, finalizzato alla gestione dei dati organizzativi, amministrativi, contabili, gestionali, fiscali, documentali all'interno degli applicativi.

CATEGORIA INTERESSATI

- Addetti azienda che utilizzano le procedure
- Clienti consumatori e potenziali clienti consumatori
- Fornitori e potenziali fornitori
- Agenti
- Collaboratori

CATEGORIE DI DATI PERSONALI

Dati anagrafici e di contatto dati bancari per il pagamento (iban), dati rivelanti la situazione economica/finanziaria.
Dati non identificabili che sono salvati nelle gestioni documentali/allegati attraverso la pubblicazione di report, scannerizzazione documenti ed estrazioni che derivano dai singoli applicativi o da fonti esterne.
I prodotti che utilizzando i suddetti dati sono:

- Gestionale Ad Hoc Infinity (completo di tutti I moduli)
- Applicativo documentale (Infinity DMS)
- Applicativo CRM (Infinity CRM)
- Applicativo portali (Infinity eCommerce)
- Applicativo Infinity Mobile App (Forza vendita, Tentata vendita)

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

Altre società del Gruppo Zucchetti – partner e subfornitori/subappaltatori, qualora la comunicazione sia necessaria per adempiere a quanto contrattualmente previsto.
Incaricati Area Supporto dei prodotti utilizzati dal Titolare per attività di assistenza e manutenzione.

TRASFERIMENTO DATI ALL'ESTERO

Non è previsto, da parte del Responsabile, il trasferimento dei dati all'estero.

VERIFICA DELLE SICUREZZE A LIVELLO APPLICATIVO

Il Titolare potrà verificare le sicurezze applicative attraverso la visualizzazione o la stampa di funzioni a ciò dedicate.

TERMINI PER LA CANCELLAZIONE DEI DATI

I termini devono essere definiti dal Cliente e l'attività di cancellazione dovrà avvenire manualmente o definita col fornitore a livello progettuale
I dati eventualmente conservati nel Data Center Zucchetti saranno conservati con le modalità contrattualizzate con il Data Center Zucchetti stesso.

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza configurabili nel sistema applicativo sono:

Gestione credenziali di accesso

- User name: l'accesso al sistema 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 impostare un intervallo temporale di validità per ciascun account oppure un numero massimo di tentativi di accesso prima dell'attivazione del CAPTCHA Block.
- Disattivazione/disabilitazione credenziali: il titolare può disabilitare le credenziali di incaricati che non hanno più le caratteristiche soggettive per accedere a quei dati personali.
- Il sistema può essere configurato con un sistema SSO.
- 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 alle singole funzioni che la compongono con il tipo di operazione eseguita
- 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

- Password: vengono registrate tramite un meccanismo di hash.
- Crypting password DB service account.
- Crittografia della base dati: La crittografia del data base SQL avviene attraverso la tecnologia TDE (Transparent Data Encryption) impostabile dal Titolare sul database server.
- Crittografia file DMS: Il Titolare può attivare la crittografia dei file generati e conservati nel DMS con tecnologia DES (valido solo soluzioni Infinity).

Privacy by default

- Attivazione profilo utente: gli utenti nell'applicativo 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 sull'applicativo e non sarà più reperibile alcuna informazione neppure indiretta su quell'interessato. In alternativa il Titolare può anonimizzare i dati personali 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 dell'applicativo c'è la possibilità di fare delle estrazioni in vari formati (CSV, XML, HTML) della parte anagrafica.

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

2. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

ASSISTENZA ON SITE

Gli addetti Zucchetti possono accedere presso la struttura del cliente per fare formazione od effettuare attività tecnica di manutenzione.
In questo caso gli addetti Zucchetti lavorano come se facessero parte della struttura del cliente ed 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 l'addetto Zucchetti abbia la necessità di prelevare archivi o db di cui necessita per risolvere le problematiche evidenziate è necessario che informi il cliente e lo registri sulla Nota di intervento.
Al termine dell'attività presso gli uffici Zucchetti il cliente sarà informato 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, il cliente dovrà essere informato 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 inserire sempre nel testo del messaggio il disclaimer:
L'addetto Zucchetti non si farà mai mandare le credenziali di accesso del cliente via email (quelle del cliente, non quelle generate appositamente per i nostri tecnici che potranno essere anche ricevute via email), né tantomeno potrà salvarle sullo strumento di ticketing.
Qualora un cliente/partner 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 gli dovremmo richiedere credenziali individuali oppure collegamento con Team Viewer.
Ogni email dovrà essere firmata con il nome e cognome dell'operatore che ha gestito il problema del cliente e salvare l'informazione nel ticketing.

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 o query contenenti dati personali è necessario comunicare al cliente o l'area ftp su cui dovrà caricare i file oppure per i clienti con l'ambiente installato sul ns. data center, richiedere l'autorizzazione per far effettuare la copia ai nostri sistemisti.

Area FTP

L'area ftp dovrà essere impostata affinché il cliente veda solo l'upload. Il download deve essere visualizzato solo dal gruppo di assistenza a cui la richiesta di assistenza è stata effettuata.
Almeno 1 volta al giorno una routine dovrà cancellare i file caricati in area ftp.

Scaricamento archivi tramite wetransfer o link di collegamento su ambienti clienti

In questo caso la gestione è in carico al cliente che ci 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 come nelle altre ipotesi.

Autorizzazione di backup da parte dei nostri sistemisti

L'archivio ricevuto dovrà essere scaricato su una directory del gruppo di assistenza non soggetta a backup.
L'assistenza di primo livello potrà trasmettere il db all'assistenza di 2 livello. L'assistenza di 2 livello dovrà procedere alle analisi di cui il problema necessita e poi dovrà cancellare gli archivi ricevuti.
In ogni caso l'assistenza che ha in carico il problema, sia essa di primo o secondo livello, dovrà preoccuparsi, al termine dell'attività, di cancellare 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 vi è la necessità di mandare una email al cliente, come di seguito:
Gli archivi dei clienti non potranno mai essere trasmessi a gruppi di lavoro differenti rispetto a quelli finalizzati alla risoluzione del problema segnalato dal cliente.
L'unica possibilità che i tecnici hanno per conservare gli archivi senza la previa autorizzazione del cliente è l'anonimizzazione degli stessi.

ASSISTENZA ATTRAVERSO LA NECESSITÀ DI AVERE IL BACKUP DEI CLIENTI DI UN SERVIZIO DATA CENTER

Qualora il cliente sia 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 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 TEAM VIEWER

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 i tecnici Zucchetti ad un ambiente con profilo di autorizzazione da lui scelto per far eseguire le attività di assistenza
- Il cliente può sconnettere 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 cliente 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 clienti:

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

REGOLE CHE RIGUARDANO GLI AMBIENTI DEI CLIENTI

Regole che riguardano gli ambienti dei clienti, 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 cliente 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 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.

Personale di Help Desk

La creazione dell'utenza deve essere richiesta solo al cliente 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

Possiamo trovarci a gestire due situazioni differenti:

- 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 cliente 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 cliente proverà la conversione

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 di svolgere tutte le attività necessarie all'erogazione del servizio.
In questo caso non serve mandare al cliente 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 cliente 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 cliente, 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 cliente ha provato 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 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 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 da noi svolto, dovremo inviare una comunicazione con la quale il cliente 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 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.

Timbro e Firma: DPO