



Autore	Ufficio privacy
Approvazione	Angelo Cian

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio privacy	06/04/2021	06/04/2021	Prima emissione

PARERE DPO Ok.



I SERVIZI E PRODOTTI ZUCCHETTI IN RELAZIONE ALLE PRESCRIZIONI DEL GDPR: TIENI IL CONTO PRO

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	Gestionali ERP	Responsabile Divisione	Giorgio Mini
Area	Soluzioni SaaS	Responsabile Reparto	Angelo Cian

INCARICATI DEL TRATTAMENTO
Responsabile prodotto e addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti, back office

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

DESCRIZIONE
<p>Tieni il Conto PRO è la soluzione gestionale in cloud completa, semplice, intuitiva, pronta all'uso ed auto esplicativa, pensata per le piccole e medie imprese che desiderano utilizzare un gestionale via web, che sia completo e allo stesso tempo immediato da avviare e molto semplice da utilizzare.</p> <p>Tieni il Conto PRO copre le seguenti aree applicative:</p> <ul style="list-style-type: none">- area Contabile (contabilità generale, scadenziari, adempimenti IVA)- moduli aggiuntivi all'area Contabile: Ritenute e Cespiti- area Vendite e Magazzino: fatturazione elettronica e ciclo attivo, provvigioni, fido clienti, movimentazioni di magazzino con gli inventari nei vari formati- moduli aggiuntivi all'area Vendite e Magazzino: Ordini



- moduli e funzionalità trasversali: Rubrica, Archivio digitale, gestione account di posta, gestione utenti e gruppi di condivisione, indicatori sull'andamento dell'azienda e sulle attività prioritarie da fare. Per utilizzare le funzionalità del software inerenti la gestione delle vendite e della contabilità in particolare, vengono censite le anagrafiche clienti, fornitori, agenti, vettori (in tutte queste anagrafiche sono contenuti dati personali).

FINALITA' DEL TRATTAMENTO

La finalità del Trattamento è legata principalmente a questi 2 aspetti:

1. erogazione dei servizi post vendita di supporto all'utilizzo dell'applicativo
2. attività di manutenzione e aggiornamento del software

CATEGORIA INTERESSATI

Addetti dell'azienda che utilizzano la procedura, Clienti, Fornitori e Agenti.

CATEGORIE DI DATI PERSONALI

Si tratta di dati identificativi di persone giuridiche e fisiche, oltre ai dati relativi alle banche d'appoggio per i pagamenti (iban) e 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.

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 (paesi Extra UE).

VERIFICA DELLE SICUREZZE A LIVELLO APPLICATIVO

Le sicurezze applicative non sono configurabili dall'utente, in quanto sono impostate di default. All'attivazione il cliente riceve una login e una password, al primo accesso gli viene subito richiesto di modificare la password.

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 conservati nel Data Center Zucchetti saranno conservati per i 90 giorni successivi alla cessazione del contratto e per ulteriori 12 mesi sottoforma di copie di backup.



DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEL SOFTWARE

Le misure di sicurezza configurabili nell'applicativo sono:

Gestione credenziali di accesso

- L'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Nel sistema c'è una credenziale c.d. Power User, che viene consegnata al titolare. 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.
- Il power user può definire nuovi utenti e la relativa profilazione, cambiare la profilazione o bloccare utenti esistenti.
- *Password*: le regole di complessità della password sono pre configurate secondo questi criteri:
 - Complessità password: è prevista una complessità minima. Il valore predefinito è 20/50 (ovvero 20 caratteri su 50). Il valore minimo richiesto è 20: se il valore è inferiore a 20, la password non viene accettata, se il valore è superiore a 20 la password viene accettata e definita come "debole", "mediocre" o "sicura" in base alla costruzione della password.
 - Giorni validità password: non viene fornito alcun valore predefinito, l'utente è libero di impostare il periodo desiderato.
 - Ciclicità password: non viene fornito alcun valore predefinito, l'utente può definire liberamente il numero di nuove password da inserire al cambio password prima di poter riutilizzare quelle vecchie.

Il power user ha la facoltà di modificare in qualsiasi momento tutti i criteri di sicurezza (complessità, validità e ciclicità) della password, tramite funzione apposita raggiungibile dal menu a tendina che si apre selezionando il pulsante in alto a destra dell'applicativo; cliccando sulla descrizione dell'"azienda installata", dalla scheda "Dati generali/Criteri di sicurezza" è possibile variare le informazioni preimpostate.

- Il Titolare ha la possibilità di disabilitare la login utente, impedendo di fatto l'accesso all'applicativo.
- Il sistema può essere configurato con un sistema SSO.
- Il Cliente ha la possibilità di modificare la propria password.

Identificazione di chi ha trattato i dati

- Strumenti di log: Il Responsabile ha attivo i log della procedura con cui sono registrati gli accessi al sistema;
- Presenza di utenze di servizio per personale di assistenza: coloro che eseguono assistenza e manutenzione sulla procedura hanno utenze nominali. La generazione temporanea del codice per l'accesso dei nostri operatori, avviene attraverso un'apposita funzionalità dove, il cliente, previo inserimento del campo "username" da noi comunicato (nominativo che effettuerà l'intervento), genera una prima parte del codice di autorizzazione. Tale parte di codice, unita ad una seconda parte (a esclusiva conoscenza Zucchetti), dà origine al codice di autorizzazione completo che consente l'accesso all'applicativo. Al termine dell'intervento dei ns. operatori, il titolare potrà disattivare il codice di autorizzazione, impedendo di fatto l'accesso dei ns. operatori. Quandanche il titolare non provvedesse alla disattivazione, il codice di autorizzazione verrà resettato automaticamente dalla procedura il giorno seguente la generazione.

Minimizzazione



- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti.

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: per ogni cliente viene utilizzato un bucket Amazon S3 (Amazon Simple Storage Service) riservato e protetto da una doppia chiave (access-key/secret-key) sicura. La comunicazione TICPRO/Amazon S3 è anch'essa sicura e crittografata, in quanto avviene utilizzando il protocollo https.

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 o di analisi presso il cliente.

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 far accedere in affiancamento per formare il loro personale.

Qualora durante l'attività di assistenza l'addetto Zucchetti abbia la necessità di effettuare copie di 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 duplicato.

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 è sempre presente uno specifico 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 L'ACCESSO AL DATA BASE DEI CLIENTI

Qualora per risolvere il problema segnalato dal cliente sia necessario accedere alla base dati o altri files o query contenenti dati personali è necessario richiedere l'autorizzazione per far effettuare la copia ai nostri sistemisti.

Autorizzazione di backup da parte dei nostri sistemisti

L'archivio 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 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.

CONVERSIONI E PROGETTI DI START UP

Le uniche attività avvengo a seguito di un contratto per cui 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.

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.



3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS - PAAS

Codice	Classe della misura	Livello di applicazione
M1	Sicurezza locali e apparati	Le aree tecniche di competenza ZUCCHETTI sono caratterizzate da misure che controllano l'accesso fisico ai locali.
M2	Autenticazione	I sistemi ed i servizi ZUCCHETTI sono accessibili solo attraverso il superamento di una procedura di autenticazione che prevede l'utilizzo di credenziali associate agli incaricati.
M3	Sistema di autorizzazione	L'accesso ai dati è controllato attraverso i profili di autorizzazione definiti a livello del sistema operativo della piattaforma che ospita l'applicazione (Windows) e a livello applicativo.
M4	Controllo integrità dei dati	Sono attivi servizi di controllo per presenza di virus sia nei file systems locali dei singoli PC che nei file system condivisi, oltre che sui messaggi di posta elettronica.
M5	Backup e Ripristino dei dati	Sono in atto politiche di backup per i dati. Sono in atto attività indirizzate a ridurre il disservizio in caso di guasto (disaster recovery)
M6	Gestione delle politiche di sicurezza	Sono predisposte delle Policy IT indirizzate alla sicurezza.
M7	Formazione degli incaricati	E' previsto un piano di formazione e di aggiornamento per gli incaricati di ZUCCHETTI.
M8	Supporti rimovibili	Sono disposte regole per la gestione (custodia, uso e riutilizzo) di supporti rimovibili in presenza di dati sensibili.
M9	Procedure automatiche di cancellazione dati utenti interni	Ci sono regole di cancellazione dei dati in relazione alle diverse attività svolte
M10	Backup	Qualora sia applicata la crittografia sul db anche i backup sono crittografati

Classificazione e scheda dettagliata delle Misure di sicurezza adottate

<i>Classe della misura</i>	<i>Misura</i>	<i>Descrizione sintetica</i>
M1.	1.1 Sistemi di allarme anti intrusione	È previsto un sistema di allarme contro le intrusioni. In caso di intrusione il sistema di allarme provvede ad avvisare automaticamente sia il servizio di guardia giurata notturno che i referenti di ZUCCHETTI



	<p>1.2 Accesso alle postazioni di lavoro e agli archivi correnti e permanenti in formato cartaceo (sistema Badge)</p>	<p>L'accesso viene consentito tramite identificazione effettuata a mezzo tesserino RFID personale (Badge) assegnato ad ogni dipendente. Le autorizzazioni di accesso alle sedi sono fornite dall'Ufficio del personale che abilita in funzione della mansione svolta o delle esigenze segnalate.</p> <p>Autorizzato l'accesso da parte dell'Ufficio del personale il lavoratore potrà accedere ad ogni orario. Unico limite temporale è relativo all'attivazione dell'impianto d'allarme che in genere avviene dopo le 22.30 e si disattiva prima delle 6.30. Qualora dovessero esserci delle esigenze particolari il lavoratore può chiedere al responsabile dell'ufficio logistica come disattivare il sistema di allarme. Il Responsabile dell'ufficio logistica, valutata l'esigenza, annoterà la richiesta e fornirà al lavoratore il codice di accesso; il Responsabile dell'Ufficio logistica provvederà il giorno successivo a modificare il codice di disattivazione.</p> <p>L'identificazione del lavoratore che accede alla sede avverrà anche in questo caso attraverso la rilevazione dell'apertura della porta.</p>
	<p>1.3 Controllo Accessi Aree Riservate</p>	<p>Per i locali a più alto rischio quali i CED di Solferino 1 e di Polenghi 9, la SERVER FARM ed i CED delle sedi remote, l'accesso agli stessi è consentito solo a personale autorizzato, previamente dotato di apposito tesserino RFID oppure destinatario di un codice numerico di accesso o di una chiave di accesso.</p>
	<p>1.4 Prevenzione incendi</p>	<p>I locali sono dotati di impianti automatici di rivelazione fumo. I locali tecnici prevedono un impianto per lo spegnimento degli incendi. Sono applicate le misure di sicurezza previste dal Dlgs 81/2008.</p>
	<p>1.5 Dislocazione degli apparati attivi e dei server di rete</p>	<p>Tutti gli apparati attivi ed i server di rete sono dislocati in locali tecnici ad accesso controllato.</p>
	<p>1.6 Registrazione accessi agli uffici</p>	<p>Data ed ora di ingresso ed uscita del personale impiegatizio vengono registrati tramite l'ausilio di apparecchi di rilevazione presenze.</p>



	1.7 Videosorveglianza	I sistemi di videosorveglianza e le relative modalità di gestione sono descritte in apposite procedure interne
M2.	2.1 Adozione di procedure di gestione delle credenziali di Autenticazione: USERNAME	<p>Tutti i lavoratori sono identificati nel sistema informativo attraverso una user name assegnata in modo univoco agli stessi.</p> <p>La User name non sarà associata ad altri lavoratori neppure in tempi diversi. Essa si compone unendo le prime tre lettere del cognome alle prime tre lettere del nome. Qualora vi sia omonimia la user verrà creata utilizzando le lettere successive o del nome o del cognome in modo da creare sempre univocità e riconoscibilità di esecuzione di trattamenti di dati personali.</p> <p>Le username si suddividono in username per accesso ad ambienti di lavoro e username per accesso alle applicazioni funzionali.</p> <p>Ogni sistema ha la propria gestione e memorizzazione della username. Solo i sistemi più strutturati, quali Infinity Portal richiedono una username per l'accesso a diverse applicazioni. Quando si accede agli strumenti informatici le username in genere sono memorizzate e riproposte all'utente all'accesso successivo.</p>
	2.2 Adozione di procedure di gestione delle credenziali di Autenticazione: PASSWORD	<p>L'accesso ad ogni ambiente o strumento elettronico avviene attraverso credenziali di autenticazione.</p> <p>La password al primo accesso viene impostata dall'ufficio tecnico che configura inizialmente l'ambiente di lavoro di ogni singolo incaricato. A seconda del sistema vengono seguite le seguenti regole:</p> <ul style="list-style-type: none"> - per l'accesso ai sistemi Novell viene impostato per il primo accesso il campo password con "cambiolapassword"; effettuato il primo accesso l'utente è obbligato a cambiare la password che sarà automaticamente impostata anche sul sistema operativo dello strumento utilizzato. - per l'accesso agli altri sistemi, viene autorizzato l'accesso con il campo password blank e viene obbligato l'utente ad inserirla al primo accesso. <p>Ogni utente che inizia un trattamento di dati personali viene edotto sull'importanza che la componente riservata della credenziale di</p>



		<p>autenticazione non venga divulgata ad altri operatori.</p> <p>Inoltre l'incaricato viene formato sulle regole minime di composizione della password (almeno 8 caratteri e costituita da caratteri alfanumerici non facilmente riconducibili al soggetto di appartenenza). Tale formazione viene effettuata con la distribuzione di un manuale informativo "Vademecum Privacy" che riporta l'indicazione anche dei recapiti dell'ufficio privacy a cui ogni operatore si potrà rivolgere per chiarimento, delucidazioni e discussioni.</p> <p>L'incaricato viene inoltre edotto sulla necessità di modifica delle password ogni sei mesi nel caso in cui tratti dati personali e ogni tre mesi qualora tratti dati sensibili (i dati giudiziari non sono stati ad oggi identificati in azienda).</p> <p>Gli strumenti utilizzati per i trattamenti spesso non gestiscono in autonomia il cambio password, né effettuano controlli sulla ripetitività delle stesse password nel tempo. Quindi tali adempimenti sono a carico dello stesso utente che assume tale onere con la sottoscrizione della lettera di incarico.</p> <p>Le password di tutti i sistemi elettronici quando vengono digitate sono in formato inintelligibile, cioè riportano asterischi e non caratteri alfanumerici.</p>
	<p>2.3 Uso esclusivo delle credenziali di autenticazione.</p>	<p>Ogni credenziale di autenticazione (username e password) viene assegnata ad un unico operatore che la utilizzerà in modo esclusivo.</p>
	<p>2.4 Disattivazione delle credenziali di autenticazione per mancato utilizzo (+ 6 mesi) o perdita qualità</p>	<p>Nel caso in cui un incaricato dovesse perdere la qualità per la quale gli erano state assegnate le credenziali di autenticazione (ad esempio cessazione dell'attività in azienda, oppure cambio di mansione di ruolo, etc). le credenziali al medesimo riferite saranno disattivate e non verranno più utilizzate. Per la casella di posta elettronica al medesimo riferita verrà osservata la procedura per l'utilizzo degli strumenti elettronici che si riporta in calce al documento. In particolare: L'USERNAME dovrà essere disattivata nei seguenti casi:</p> <p>Immediatamente, nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere allo</p>



		<p>strumento (sia nel caso in cui cessi di lavorare, sia nel caso in cui venga trasferito da un ufficio ad un altro con conseguente cambio di mansioni e di ambiti di trattamento dei dati personali tale da rendere necessario il conferimento di una nuova chiave);</p> <p>In ogni caso, entro sei mesi di mancato utilizzo.</p>
	2.5 Verifica delle credenziali	<p>Tutte le credenziali sono verificate con cadenza annuale, in occasione della redazione della DPIA, al fine di controllarne l'effettiva corrispondenza con le mansioni effettivamente svolte.</p>
	2.6 Divieto di lasciare incustodita la postazione di lavoro durante una sessione di trattamento.	<p>L'incaricato viene edotto circa la necessità di non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento. Detta regola potrà essere disattesa solo alla presenza contestuale delle seguenti condizioni:</p> <ul style="list-style-type: none"> * prolungata assenza o impedimento dell'incaricato; * l'intervento è indispensabile ed indifferibile; * presenza di concrete necessità di operatività e sicurezza del sistema; <p>In tal caso dell'accesso effettuato si dovrà provvedere ad informare tempestivamente l'incaricato cui appartiene la parola chiave.</p>
M3	3.1 Profilo di autorizzazione per singolo incaricato	<p>Detto processo garantisce, a fronte del superamento della fase di autenticazione, la corretta e completa associazione tra utenza ed oggetti del sistema informatico connessi al profilo assegnato; comprende l'insieme delle informazioni, associate ad una persona, dirette ad individuare a quali dati essa possa accedere ed altresì di quali trattamenti essa possa usufruire; esso stabilisce a quali aree del sistema informatico l'incaricato possa accedere e quali azioni, una volta entrato, possa compiere.</p>
	3.2 Aggiornamento periodico dei profili di autorizzazione	<p>Ad ogni incaricato, prima di iniziare il trattamento, viene configurato un profilo di autorizzazione. Il profilo di autorizzazione viene configurato dal coordinatore del gruppo di lavoro di cui la risorsa farà parte, valutando profili analoghi di colleghi che prestano la stessa attività professionale ed evidenziando le eccezioni. I profili di autorizzazione vengono configurati da parte del coordinatore inviando una email reimpostata con un modello</p>



		<p>all'ufficio tecnico che provvede ad implementare i livelli di autorizzazione o direttamente o trasmettendo l'informazione ai rispettivi responsabili di prodotto per l'attivazione del profilo di autorizzazione delle singole applicazioni. Se in corso di rapporto di lavoro viene valutata l'esigenza di estendere o restringere il profilo di autorizzazione, sarà il coordinatore ad inviare la comunicazione all'ufficio tecnico o ai singoli responsabili di prodotto al fine di provvedere a tale adempimento.</p>
M4	4.1 Architettura sicurezza informatica	<p>È previsto un insieme di regole comportamentali e procedure operative dirette a proteggere l'intero sistema informatico.</p> <p>In particolare, esso prevede l'adozione di programmi diretti a prevenire la vulnerabilità degli strumenti elettronici da un lato contrastando gli attacchi esterni dall'altro provvedendo alla correzione dei difetti insiti negli strumenti stessi.</p> <p>In relazione alla correzione dei difetti, esso opera l'aggiornamento costante dei prodotti e la verifica periodica dell'installazione e della configurazione dei prodotti software.</p> <p>In relazione alla tutela da intrusioni esterne di iniziativa della "mente criminale", l'architettura antivirus si serve di sistemi IDS (Intrusion Detection System), gestiti dal gruppo Sistemistico di Zucchetti, diretti ad individuare qualunque tentativo di operare e/o introdursi illecitamente nella rete e nei sistemi posti sotto protezione.</p> <p>Gli stessi devono svolgere almeno le seguenti funzioni:</p> <ul style="list-style-type: none"> * analizzare il traffico di rete secondo i modelli predefiniti dall'amministratore allo scopo di rilevare attività anomale; * effettuare un'attività di log molto dettagliata; * segnalare immediatamente i tentativi di intrusione ed eventualmente intervenire automaticamente con le opportune contromisure. <p>E' attivo un sistema antivirus che monitorizza tutta la rete aziendale (MCAfee). Il sistema è attivo sia sui desktop che sui laptop della sede di Lodi e delle sedi</p>



		<p>periferiche. L'antivirus si aggiorna tutte le volte che la casa produttrice aggiorna la lista delle segnalazioni virus. L'ufficio tecnico, qualora ritenga che a seguito di richiesta di un operatore, il sistema possa essere infetto, lancia la scansione per verificare eventuali infezioni. I laptop sono muniti di sistema antivirus (McAfee) che si aggiorna tutte le volte che il laptop si collega alla rete aziendale. Vi è un sistema di firewall che filtra le comunicazioni in entrata e in uscita.</p>
M5	5.1 Procedure di backup	<p>Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera.</p>
	5.2 Procedure di ripristino	<p>Sono adottate idonee misure atte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni. Sono altresì previste attività indirizzate a ridurre il disservizio in caso di guasto.</p>
M6	6.1 Policy per l'utilizzo degli strumenti IT	<p>Sono predisposte policy per l'utilizzo degli strumenti elettronici relativamente agli aspetti di:</p> <ul style="list-style-type: none"> - Utilizzo del Pc; - Navigazione internet - Utilizzo della posta elettronica <p>La responsabilità di gestione delle stesse è affidata all'Ufficio Tecnico sezione Sicurezza.</p>
M7	7.1 Piano di Formazione degli incaricati	<p>E' previsto un piano di formazione e di aggiornamento per gli incaricati ZUCCHETTI. A tutti i neoassunti apprendisti viene erogata una formazione di 6 ore sulla disciplina prevista dalla normativa privacy e sulle relative problematiche di applicazione. In occasione dell'inserimento di nuovi strumenti o standard aziendali viene effettuata una formazione a coloro che dovranno applicarli o utilizzarli.</p> <p>E' stato costituito un settore aziendale, Accademia Zucchetti, che è incaricato di evadere le richieste formative provenienti dai diversi settori o divisioni di gruppo.</p>



M8	8.1 Istruzioni agli incaricati	Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
	8.2 Custodia, uso e riutilizzo supporti rimovibili	I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intellegibili e tecnicamente in alcun modo ricostruibili.
M9	9.1 Procedure automatiche di cancellazione dei dati	<p>Ci sono procedure automatiche di cancellazione dei dati nei seguenti casi:</p> <ul style="list-style-type: none"> • Videosorveglianza: nelle sedi in cui sono attivi sistemi di videosorveglianza i dati videoripresi vengono cancellati entro 7 giorni dalla loro ripresa in automatico dal sistema di registrazione. Il termine è stato valutato in funzione del fatto che gli impianti sono attivi solo in orario notturno e spesso non contengono dati personali perché riprendono aree non frequentate. • Navigazione in internet: i files dei log della navigazione in internet vengono automaticamente cancellati ogni 6 mesi. I log custodiscono informazioni riconducibili a persone fisiche solo indirettamente, infatti i log registrano le attività di navigazione effettuate da gruppi di lavoro e solo a seguito di segnalazione di anomalia i log vengono impostati per registrare gli accessi ad internet dei singoli operatori. • Posta elettronica: le caselle email degli operatori vengono conservate per un periodo di 30 giorni successivo alla cessazione del relativo rapporto di lavoro. Ciò al fine di tutelare le attività svolte e di continuare a gestire i rapporti sospesi con clienti e altri gruppi di lavoro. • Dismissione strumenti elettronici: ogni strumento elettronico da dismettere viene inviata all'ufficio tecnico al fine di valutarne la reale cessazione del ciclo di vita. Se l'addetto dell'ufficio tecnico valuta che lo strumento elettronico deve essere dismesso, prima di consegnarlo allo smaltitore o



		<p>all'acquirente esterno, formatta i dischi di memoria.</p> <ul style="list-style-type: none"> • Distruzione supporti rimovibili: i supporti rimovibili quando cessano il loro ciclo di vita vengono fisicamente distrutti.
M10	10.1 Backup	<p>Qualora la base dati è crittografata anche i backup sono crittografati. E' implementato un sistema di cifratura dei backup dei servizi di DC</p>

4. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA APPLICATE AL DATA CENTER

- **Certificazioni:** Zucchetti ritiene la sicurezza un elemento prioritario e irrinunciabile per l'azienda e per i propri clienti per questo ha organizzato i propri sistemi di gestione in modo da seguire rigidi criteri di sicurezza. L'organizzazione di un sistema di gestione impone la creazione di ruoli, flussi di attività e procedure chiaramente definiti a presidio dei processi aziendali. Certificazioni: ISO 9001 e ISO 27001
- **Compliance:** i processi aziendali di Zucchetti rispondono alle normative vigenti, in particolare per quanto riguarda la rispondenza ai requisiti di privacy. In tale ambito l'azienda ha adeguato il proprio sistema di gestione alle richieste del provvedimento del Garante per la Protezione dei Dati Personali riguardo gli amministratori di sistema. Qualora le prescrizioni di legge vengano modificate Zucchetti adeguerà immediatamente le modalità di erogazione del servizio e le caratteristiche tecniche per essere conforme alle eventuali modifiche.
- **Accesso alle informazioni:** il sistema di gestione di Zucchetti prevede l'esplicita classificazione del livello di riservatezza di ogni documento. In particolare i documenti contenenti informazioni sui sistemi di sicurezza vengono classificati come riservati e non sono diffusi all'esterno dell'azienda.
- **Accesso ai sistemi:** gli accessi ai sistemi sono sempre classificabili in accessi di produzione e accessi di amministrazione. Gli accessi di produzione sono quelli oggetto della fornitura del servizio. Gli accessi di amministrazione sono quelli effettuati da Zucchetti o dal cliente con finalità diverse quali la manutenzione, la verifica di anomalie, l'acquisizione di dati. Gli accessi di amministrazione da parte di Zucchetti sono riservati a personale con la qualifica ("ruolo") di amministratore di sistema. L'azienda pone particolare attenzione all'assegnazione di tale ruolo soltanto a personale di elevate capacità tecniche e avente caratteristiche di comprovata affidabilità e moralità. L'accesso amministrativo ai sistemi da parte di personale del cliente avverrà attraverso l'assegnazione nominale di personale a ruoli ai quali sono assegnati privilegi di accesso.
- **Auditing:** nell'ambito del proprio sistema di gestione Zucchetti pone particolare attenzione all'audit dei sistemi e delle attività amministrative compiute sugli stessi. Ogni sistema viene configurato per riportare i propri log verso un sistema centralizzato di elaborazione, classificazione e repository. Tale sistema è in grado di rilevare in tempo reale anomalie sui



sistemi. In particolare sono riscontrabili sia eventi singoli che pattern di attività anomale quali serie di login fallite, modifiche massive di permessi o di password. Il sistema di gestione e analisi dei log viene inoltre utilizzato per il monitoraggio delle attività degli amministratori di sistema come prescritto dal provvedimento del Garante per la privacy. L'accesso al sistema di gestione dei log è riservato al personale di Zucchetti avente ruolo di auditor ed è inaccessibile al personale addetto all'amministrazione di sistema.

- **Riservatezza dei dati:** il presente documento è stato prodotto assumendo che i dati raccolti dal cliente e presenti sui sistemi ospitati all'interno del Datacenter siano di tipo personale/sensibile, secondo la classificazione prevista dal Regolamento UE 2016/679 in materia di protezione dei dati personali. In ogni caso Zucchetti non tratterà i dati del Cliente se non per l'unica finalità della loro conservazione. Zucchetti non potrà conoscere in nessun modo i dati personali inseriti dal cliente se non previa sua autorizzazione finalizzata all'esecuzione di attività di manutenzione e assistenza dell'ambiente. Zucchetti non si assume alcuna responsabilità riguardo all'uso che di tali dati viene fatto da parte del cliente o da società incaricate dal cliente stesso che gestiscono o utilizzano il servizio ubicato e gestito nel Datacenter. Zucchetti gestirà e conserverà le informazioni in conformità alle norme espresse dal Regolamento Ue 2016/679
- **Log Management:** i log dei sistemi contengono informazioni necessarie alle attività amministrative, di diagnostica e di sicurezza. Ogni sistema viene configurato per loggare ogni evento significativo. I log generati da ogni sistema vengono trasferiti ad un repository centrale che ha il compito di analisi, classificazione e storage. La conservazione dei log avviene secondo le norme di legge, in particolare il Codice Privacy e le norme sulla conservazione dei dati di traffico telefonico e telematico. I log dei sistemi riportano tutte le attività significative ai fini della sicurezza quali gli accessi amministrativi, le modifiche ai permessi e alle configurazioni di sistema e di sicurezza, le anomalie. Tali log sono conservati con le stesse modalità dei log di sistema. In particolare sono tracciate ed archiviate tutte le attività di accesso e amministrazione in conformità al provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 riguardo gli amministratori di sistema. Il sistema di repository dei log è in grado di generare alert sulla base di eventi o pattern di eventi anomali.
- **Crittografia dei dati:** non sono presenti sistemi di crittografia sui dati poiché per la tipologia trattata non è prevista in quanto non si tratta di dati sensibili. E' prevista crittografia soltanto sulle password di accesso ai vari sistemi.
- **Sicurezza dei sistemi:** i servizi di sicurezza si ritengono attivi e funzionanti a protezione delle componenti ospitate in Datacenter. I sistemi di protezione sono progettati in modo da massimizzare la protezione e sono amministrati da personale con formazione specifica che segue procedure operative stringenti.
- **Controlli di sicurezza:** sull'intera infrastruttura Datacenter sono svolti Penetration Test e Vulnerability Assessment con cadenza annuale
- **Firewalling:** il networking del Datacenter è separato dalle reti pubbliche, dalle altre reti di Zucchetti e dalle altre reti del cliente. I flussi dati tra il networking del Datacenter e l'esterno



vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati.

- **Intrusion Prevention:** il Datacenter è protetto da sistemi di Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito e si comportano in modo trasparente nei confronti del traffico legittimo.
- **Filesystem Antivirus:** tutti i server dispongono di moduli Antivirus sul filesystem e, su base progettuale, possono essere configurati prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.
- **Security Patch Management:** la piattaforma è sottoposta ad un processo periodico di verifica delle patch o delle fix rilasciate dal produttore e ritenute critiche per l'erogazione del servizio o per la sicurezza. L'applicazione delle patch verrà sottoposta a preventiva comunicazione al cliente e la schedulazione avverrà in accordo con quest'ultimo.
- **Sicurezza fisica:** la piattaforma hardware/software progettata fruisce di tutti i servizi di facility management del Datacenter. Di seguito sono evidenziati i 2 più importanti: rilevazione fumi e spegnimento incendi. Tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio, con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguento chimico gassoso FM-200. Gli impianti garantiscono la sola disattivazione della zona oggetto dell'intervento di manutenzione. In particolare, l'impianto di spegnimento è stato progettato nel pieno rispetto della normativa UNI 9795 che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente, o calamità naturale, ed il continuo funzionamento del resto dell'impianto.
- **Anti allagamento:** sono previste delle sonde di rivelazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua. Eventuali fuori uscite di acqua saranno opportunamente allontanate mediante convogliamento e scarico verso l'esterno.
- **Anti intrusione:** è previsto un sistema di anti intrusione integrato con l'impianto di rivelazione fumi e spegnimento incendi, con il sistema di TVCC, con il sistema di controllo accessi e con gli allarmi tecnologici. I sensori del sistema allocati all'interno dell'edificio saranno attivati e disattivati da segnali provenienti dal sistema di controllo accessi.
- **Telecamere a circuito chiuso:** le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.
- **Condizionamento:** nei Datacenter di ultima generazione tutti gli impianti di condizionamento e di raffreddamento sono concepiti per poter smaltire tutta l'energia elettrica assorbita. Il limite massimo di energia termica smaltibile (media nell'area) è 2898 BTU/h per ogni metro quadro; la temperatura standard del Datacenter oscilla fra i 21 ed i 23 °C, con tolleranze di +/- 1°C.



- Continuità ed emergenza: il Datacenter è stato concepito per fornire affidabilità massima in termini di alimentazione dei server, in quanto ogni rack è connesso a due alimentazioni indipendenti (quadri elettrici attestati su UPS ridondati), in modo tale da permettere la manutenzione delle singole linee di alimentazione senza creare disservizio e di scongiurare black-out nel caso di fault di una linea di alimentazione. Gli interventi di manutenzione programmata comportano un fermo sulle singole alimentazioni, stimabile in circa 2 ore annue complessive. La ridondanza dell'alimentazione è ulteriormente garantita da una serie di batterie, che, nel caso di black-out di entrambe le linee di alimentazione, permettono di erogare corrente ai server per 45 minuti; in realtà tali batterie intervengono semplicemente per il tempo strettamente necessario (circa un minuto) all'entrata in regime del gruppo elettrogeno a gasolio, che ha un'autonomia di 36 ore.
- Controllo degli accessi fisici al Datacenter: sorveglianza armata 24 ore su 24, procedure di registrazione degli accessi e identificazione del personale che accede in nome e per conto dei clienti, accesso alle sale sistemi controllato elettronicamente tramite badge e sistemi di rilevamento di impronte digitali, controllo del perimetro con impianti a raggi infrarossi, test periodici di evacuazione, procedure di sicurezza con identificazione ed assegnazione di responsabilità.

Connettività del Datacenter

- Linee Internet: l'ampiezza di banda è in grado di fornire il massimo delle performance in ogni circostanza. Ad oggi, al fine di assicurare funzionalità piena anche in caso di malfunzionamenti delle linee Internet di un Provider, il Data Center Zucchetti è collegato in fibra ottica con diversi fornitori di connettività e con capacità superiore ai 2 Gbit/s.
- Disponibilità di banda: la disponibilità di banda è garantita da monitoraggio continuativo 24x7, 365 giorni l'anno. Ogni cliente dispone di un quantitativo di banda pari al nr. di Mbit/s contrattualizzato. Tale numero rappresenta la soglia massima di banda utilizzabile senza applicare filtri e/o blocchi sulla comunicazione, permettendo di gestire in modo dinamico eventuali picchi sul servizio erogato. Qualora il cliente superi tali "soglie" è necessario rivalutare il quantitativo di banda disponibile per la pubblicazione e/o per l'erogazione di un servizio internet.
- IP pubblici: Zucchetti, in qualità di Autonomous System, è in grado di offrire ip pubblici senza limitazioni e ha, qualora sia necessario, la possibilità di utilizzare gli indirizzamenti di proprietà del cliente.
- Routing: tutte le funzioni di routing sono garantite da apparati ridondati e configurati in modalità HSRP (Hot stand-by Routing Protocol) ove il secondario rimane in hot standby ed in grado di attivarsi automaticamente al verificarsi di un fault sul router/link primario.
- Firewalling: il servizio è gestito tramite sistemi ridondati al 100% prodotti da primari produttori HW internazionali. Gli stessi sono configurati in high availability in modalità Active/Passive usando il metodo LAN-Based Stateful. La sicurezza logica è garantita sia a livello perimetrale che



tra i sistemi di front-end e il back-end. Sono applicate policy globali per l'inspection dei pacchetti applicando class map standard.

- Firewall Perimetrale: i sistemi di firewall perimetrale proteggono il Datacenter Zucchetti dalle minacce provenienti dal mondo Internet. Utilizzando le migliori tecnologie presenti sul mercato sono in grado di garantire, in ogni momento, la massima fruibilità e protezione per i servizi esposti sul web. Il servizio è ridondato in ogni suo componente, assicurando così una continua disponibilità dei sistemi.
- Firewall di back end: i firewall di backend forniscono un'ulteriore protezione per i dati presenti all'interno del Datacenter Zucchetti. Tali dispositivi garantiscono l'integrità e la confidenzialità degli archivi presenti sui server di backend (database, file server ...). Il servizio, ridondato in ogni suo componente, è in grado di fornire le massime performance abbinate alla massima disponibilità.
- Sistema anti-intrusione: identifica l'insieme delle strumentazioni hardware e delle configurazioni software che permettono di "tracciare" l'accesso a particolari servizi e fornire, su richiesta, l'elenco degli accessi effettuati su un particolare sistema e/o un particolare servizio.
- AntiDDoS: Il Datacenter Zucchetti sfrutta un servizio offerto da: BT, incluso nella linea internet con protezione L4; FASTWEB, con un servizio ad alto profilo tecnologico che permette di rispondere in modo efficace alle problematiche create dagli attacchi DDoS.
- IDS: nel Datacenter Zucchetti è presente un sistema IDS (Intrusion Detection System). Questo dispositivo è in grado di individuare e segnalare in tempo reale i tentativi di accesso non autorizzato. Il sistema, aggiornato in tempo reale da migliaia di sensori presenti in tutto il pianeta, è in grado di rilevare la quasi totalità delle minacce provenienti da internet (attacchi da parte di Hacker, Virus ecc...)
- IPS : il sistema IPS (Intrusion Prevention System) è in grado di bloccare automaticamente gli attacchi rilevati dal dispositivo IDS, fornendo così una protezione real-time ai servizi erogati dal Datacenter Zucchetti.
- Linee di comunicazione: le soluzioni ed i servizi proposti possono essere erogati tramite connessione Internet protetta (https). Il cliente potrà scegliere di predisporre a propria cura e spese una linea di comunicazione VPN o MPLS. Si tenga conto che, per le applicazioni della Suite HR Zucchetti interamente "web based" e predisposte per il controllo interno dei criteri di sicurezza, non ci sono significative differenze tra l'utilizzo attraverso le linee dedicate (VPN o MPLS) e l'accesso tramite connessione Internet protetta.