REGISTRO DEI TRATTAMENTI "RESPONSABILE DEL TRATTAMENTO" FALLCOWEB

RESPONSABILE DEL TRATTAMENTO					
Denominazione	**Zucchetti Software Giuridico Srl**				
Partita Iva	02667520247				
Indirizzo	Via Enrico Fermi, 134				
Città	Vicenza	Cap	36100	PV	VI
Legale Rappresentante	**Vasco Ciresola**				

STRUTTURA ORGANIZZATIVA			
Divisione	Software Giuridici	Responsabile Divisione	Vasco Ciresola

INCARICATI DEL TRATTAMENTO
Addetti area commerciale Addetti area amministrativa Addetti area tecnica (Programmatori, Sistemisti) Addetti area assistenza (settore Help desker- servizio clienti, settore Back Office) Risorse presenti nei Tribunali

DATI DI CONTATTO			
Responsabile protezione dati (DPO)	**Mario Brocca**	ufficio.privacy@zucchetti.it	0371/594.3191

DESCRIZIONE
FallcoWEB è la piattaforma progettata e realizzata per la gestione: -del crm in cui sono gestite le anagrafiche dei clienti e potenziali ed il relativo aggiornamento; -dei sw della linea Fallco quali Fallco Fallimenti, Fallco Esecuzioni, Fallco Hub, Fallco Legale, Fallco Ctu, Fallco Anatocismo, Fallco Revocatorie, Fallco Gestore Crisi, Fallco OCC, Fallco Mail, Pec ZetaMail, Redattore atti per PCT, Virtual Data Room e Sito del Curatore a cui accedono i clienti in funzione dei servizi che hanno acquistato; -dei siti internet dedicati alle esposizioni al pubblico delle liste delle procedure concorsuali, nonchè dell'area creditore dedicata alla consultazione documentale afferente il credito messa a disposizione da parte dei curatori. - del servizio di prenotazione online degli appuntamenti presso la Cancelleria della IX Sezione Civile - Ufficio del Giudice Tutelare di Roma riservato agli avvocati, agli amministratori di sostegno, ai tutori, ai curatori, alle persone amministrate e ai prossimi congiunti delle medesime, oltre ai responsabili dei servizi sociali o sanitari interessati ai singoli procedimenti. Quali servizi correlati ai prodotti sopra riportati sono previsti: -l'attività di assistenza post vendita che implica la lettura dei dati dall'archivio cliente (database, stampe…); -per il servizio di deposito degli atti telematici al PCT è data la possibilità al professionista di integrare la propria PEC (fornita da terzi) nei sw per inviare il deposito e ricevere le notifiche ed i biglietti di cancelleria direttamente dall'interfaccia dei programmi; pertanto la casella pec viene scansionata periodicamente dal sw al fine di trovare le suddette comunicazioni; - l'inserimento di anagrafiche, coinvolte nei gruppi di lavoro, dei collaboratori dei professionisti; - il servizio di data entry che prevede l'importazione dati dall'archivio cliente (file excel, csv …) per l'acquisizione nella piattaforma FallcoWeb; -attività di "outsourcing" software e gestione dei dati per coadiuvare gli organi che gestiscono grandi procedure concorsuali. Oltre a quanto sopra riportato, Zucchetti Software Giuridico offre un servizio IR concernente l'esame della documentazione di riconoscimento del cliente con attestazione della sua identità, il caricamento dei documenti sul gestionale del fornitore ed il rilascio al cliente della ricevuta al fine ottenere la firma digitale.

FINALITA' DEL TRATTAMENTO

Gestione dell'informatizzazione delle procedure concorsuali, esecutive (immobiliari e mobiliari) e di sovraindebitamento; gestione dei depositi degli atti telematici al PCT; ricezione delle notifiche dei depositi PCT e dei biglietti di cancelleria; consultazione dei registri informatizzati di Cancelleria e del REGINDE; gestione delle comunicazioni a mezzo PEC; gestione della fatturazione elettronica attiva e passiva; gestione analisi conti correnti per calcolare i versamenti di natura solutoria, con riferimento al saldo disponibile, tenendo conto dei vari tipi di operazioni compiute e per evidenziare i fenomeni di anatocismo ed usura; gestione della conservazione dei dati relativi alle prenotazioni presso la Cancelleria di Roma.

CATEGORIA INTERESSATI

Soggetti debitori/creditori; professionisti coinvolti nelle procedure concorsuali, Giudici Delegati, Cancellieri; professionisti delegati alla vendita, custodi giudiziari e professionisti delegati agli adempimenti successivi all'aggiudicazione; professionisti gestori della crisi, liquidatori ed indebitati; avvocati, periti; offerenti d'asta; gli amministratori di sostegno, i tutori, le persone amministrate e i prossimi congiunti delle medesime, responsabili dei servizi sociali o sanitari interessati ai singoli procedimenti presso la Cancelleria di Roma.

CATEGORIE DI DATI PERSONALI

Dati anagrafici; documenti afferenti il credito spettante; dati di contatto; dati bancari e contabili; documenti predisposti dal Tribunale; dati giudiziari.

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

Il responsabile del trattamento si avvale di fornitori di servizi che svolgono funzioni strettamente connesse e strumentali all'operatività, anche tecnica, delle applicazioni, quali: aziende del Gruppo Zucchetti Spa per la fornitura di data center, fatturazione elettronica e conservazione sostitutiva, funzione di Punto di Accesso per la consultazione del fascicolo telematico come conservato in Siecic. Il responsabile del trattamento si avvale inoltre di fornitori di: pec, servizio di Analisi di Bilancio, richiesta di documenti/visure camerali, visure pec e depositi telematici al Registro Imprese. Ulteriori destinatari cui possono essere comunicati i dati sono i Tribunali ed enti pubblici.

TRASFERIMENTO DATI ALL'ESTERO

I servizi data center a scopo di backup dei file sono in Irlanda. Viene utilizzato il fornitore Google per la gestione delle mail e per la trasmissione dei files. Come da dichiarazione del produttore non si conosce dove risiedono i dati ma il fornitore afferma di garantire la compliance rispetto alla normativa europea.

STRUMENTI ELETTRONICI UTILIZZATI NEL TRATTAMENTO

Strumenti elettronici quali pc laptop, computer desktop, server, pec, email ordinaria, SSD, memory Key USB, memory card, CD-ROM e DVD-ROM, hard disk (interni ed esterni), memorie dei cellulari, tablet, drive cloud.

TERMINI PER LA CANCELLAZIONE DEI DATI

I tempi di conservazione dei dati sono differenti a seconda del processo di trattamento:
-I dati immessi nei sw della linea Fallco, tenendo conto della tecnologia disponibile e dei mezzi a disposizione, non vengono cancellati.
-Attualmente il dato amministrativo del cliente inserito nel crm non viene cancellato ma archiviato. Prossimamente è prevista la cancellazione del dato dopo 10 anni dalla chiusura dell'ultimo rapporto amministrativo contabile attivo.
-I dati ricevuti tramite PEC dei servizi Fallco Mail e Pec ZetaMail sono cancellati dallo strumento di posta dopo essere stati scaricati nella procedura.
-I dati dei professionisti esaminati per il servizio IR vengono cancellati dopo un anno dal recepimento degli stessi.
-I dati anagrafici dei creditori registrati sui portali loro dedicati attualmente non vengono cancellati. Prossimamente è prevista la cancellazione del dato dopo 10 anni dalla chiusura dell'ultima procedura concorsuale.
-I dati allegati allo strumento di ticket vengono cancellati dopo 30 giorni dalla chiusura del medesimo.
-I dati trasmessi all'Area assistenza e alle Sezioni back office vengono cancellati dopo 30 giorni dal termine dell'intervento.
-I dati relativi al servizio di prenotazione presso la cancelleria del Tribunale di Roma vengono cancellati dopo 5 anni

dall'evento prenotazione.
- Per i dati ricevuti tramite email e PEC non è prevista una procedura di cancellazione. Premesso che all'interno degli archivi mail/pec è presente uno storico di informazioni di natura tecnica necessarie al buon svolgimento all'attività lavorativa, l'azienda ritiene utile il mantenimento di tale archivio ed eccessivamente oneroso imporre al dipendente una cernita tra le comunicazioni con dati personali da cancellare e quelle invece da mantenere. Inoltre l'azienda ritiene che i dati che tratta costituiscano adempimento previsto dalla legge e come tali non sono soggetti alle regole previste per il trattamento dei dati personali.

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:

- User name: le credenziali di accesso sono generate dai tecnici di assistenza all'atto di creazione dell'account. Per alcune procedure sono create anche credenziali per i tecnici di assistenza per seguire la procedura ed aiutare il titolare nella gestione del sistema. Il sistema non consente la generazione di utenti uguali;
- Qualora vi fosse la necessità per i tecnici di accedere con utenze dei clienti, nel sistema è prevista la tracciatura di accesso individuale del tecnico che utilizza l'utenza del cliente;
- Gli accessi delle utenze amministrative sono loggati e conservati in formato che garantisce l'integrità degli stessi. I log sono conservati per 1 anno;
- Password: le regole di complessità della password non sono configurabili nel sistema da parte del titolare. Le password non possono essere più corte di 8 caratteri;
- Sostituzione delle password per tutti al primo accesso;
- Le policy delle password dovranno essere complesse: numero caratteri, alfanumerici, caratteri speciali;
- Ogni utente è tenuto a cambiare la password ogni 6 mesi e la nuova password deve essere diversa dalla precedente;
- Strumenti di log: Il log della procedura registra gli accessi alla procedura e alle singole funzioni che la compongono con il tipo di operazione eseguita;
- Tutti gli output generati dalla procedura sono loggati ed identificano l'utente che ha fatto l'esportazione;
- 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;
- Crittografia delle password: viene registrato un hash delle password aggiungendo un "salt";
- Attivazione profilo utente "gruppo di lavoro". Sarà il Titolare a scegliere la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale;
- Diritti degli interessati: per garantire all'interessato il diritto all'oblio di un documento/informazione analitica di pubblica consultazione che riporta suoi dati (es. documentazione giudiziaria) è sufficiente che invii una richiesta al Titolare del trattamento che farà le opportune valutazioni. Qualora il Titolare decida che i dati debbano essere cancellati, ZSG darà assistenza tecnica nella rimozione del documento/informazione analitica oggetto di richiesta dall'area pubblica dei portali. Con cadenza giornaliera in automatico vengono posti a disposizione dei motori di ricerca di internet (es. google) un ricalcolo e una rigenerazione dei dati che possono essere oggetto di ricerca;
- Stampe ed estrazioni per evidenziare i dati degli interessati forniti dagli stessi e trattati nel sw;
- Ogni criticità di sicurezza è risolta tempestivamente con patch applicate al software e con l'applicazione di aggiornamenti di sicurezza a tutti i software terzi installati.

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

ASSISTENZA ON SITE

Gli addetti Zucchetti Software Giuridico accedono presso la struttura del Titolare per fare formazione od effettuare attività di assistenza post vendita.
In questo caso gli addetti accedono come se fossero parte della struttura del Titolare ed adottano tutte le procedure che il

cliente richiede di applicare.

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 l'addetto Zucchetti inserirà 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 email 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.
Gli addetti Zucchetti firmeranno ogni email con nome e cognome.

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 di utilizzare per la trasmissione dei suddetti esclusivamente l'area wetransfer oppure il servizio di tickets web.

Area wetransfer

L'area wetransfer è impostata affinchè il Titolare veda solo l'upload. Il download deve essere visualizzato solo dal gruppo di assistenza a cui la richiesta di assistenza è stata effettuata.
Gli archivi trasmessi dovranno essere scaricati in dischi di rete non soggetti a backup e cancellati dopo 30 giorni dal termine dell'attività. Nel caso in cui il Titolare contesti l'operato entro il suddetto termine, l'archivio dovrà essere conservato per ulteriori 30 giorni, decorsi i quali senza ulteriori osservazioni dovrà essere cancellato.

Area tickets web

Qualora un Titolare necessiti di trasmettere files attraverso lo strumento di ticket viene avvertito che nel testo del medesimo non dovranno essere inseriti dati personali, anche di natura sensibile, in quanto il ticket non è oggetto di procedure di cancellazione. Il Titolare è pertanto invitato ad inserire tali dati esclusivamente negli allegati, che saranno automaticamente eliminati dopo 30 giorni dalla chiusura del ticket.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO CON FUNZIONI DI FALLCO

Gli addetti Zucchetti che eseguono attività di assistenza che necessiti della visualizzazione dell'ambiente del Titolare possono accedere al DB attraverso l'abilitazione concessa dal medesimo che crea un range di date per l'accesso.
L'autorizzazione viene data tramite una maschera in Fallco, che viene lanciata dal cliente; l'attività di assistenza dura fino a che il Titolare non interrompe la sessione.

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

- Il collegamento è sempre richiesto dal Titolare
- Il Titolare può disconnettere l'addetto Zucchetti quando desidera.

Durante queste attività l'impersonificazione degli addetti viene loggata.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO TEAM VIEWER

Questa modalità di collegamento sugli strumenti dei Titolari viene utilizzata esclusivamente per la risoluzione di problematiche relative al funzionamento dei dispositivi di firma digitale dei Titolari e 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.

ASSISTENZA TRAMITE CHAT

Non presenta problemi da un punto di vista di trattamento di dati personali poiché la chat viene utilizzata esclusivamente per la risoluzione di problematiche relative al funzionamento dei dispositivi di firma digitale dei clienti. Non sono pertanto trasmessi dati o archivi.

IMPORT DI DATA BASE DEI CLIENTI

L'attività di importazione è finalizzata al completamento del servizio SAAS erogato.
La trasmissione degli archivi da importare da parte del Titolare è configurabile quale consenso espresso da parte sua ad eseguire l'attività.

ASSISTENZA "GRANDI PROCEDURE"

Gli addetti Zucchetti possono gestire dei dati in outsourcing per conto di grandi procedure concorsuali.
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; le attività sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite.
Al termine di ogni attività concordata è prevista una rendicontazione di quanto svolto e contestuale richiesta di collaudo da parte del Titolare entro 30 giorni; allo scadere del predetto termine, in assenza di osservazioni, ogni archivio trasmesso dal Titolare verrà eliminato.
Tutto l'iter svolto dovrà essere inserito nel post vendita al fine di averne memoria in caso di necessità.
Tutti i documenti contenenti dati personali dei Titolari stampati non possono essere riutilizzati come carta da riciclo e devono essere distrutti per mezzo del tritadocumenti prima dello smaltimento della carta.
Per effettuare tutte le attività di assistenza "grandi procedure" sull'ambiente del Titolare è necessario che venga appositamente creata un'utenza all'interno del sistema come di seguito indicato:
Zucchetti_+ prima lettera nome + prima lettera cognome
In questo modo il Titolare potrà riconoscere la provenienza dell'utenza stessa.
Es: per il soggetto Rossi Mario dovrà essere creata l'utenza: Zucchetti_MR

3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER GLI INCARICATI DI ZUCCHETTI SOFTWARE GIURIDICO

CODICE	CLASSE DELLA MISURA	LIVELLO DI APPLICAZIONE
A	Sicurezza locali e apparati	Le aree tecniche di competenza ZSG sono caratterizzate da misure che controllano l'accesso fisico ai locali.
B	Autenticazione	I sistemi ed i servizi ZSG sono accessibili solo attraverso il superamento di una procedura di autenticazione che prevede l'utilizzo di credenziali associate agli incaricati.
C	Sistema di autorizzazione	L'accesso ai dati è controllato attraverso i profili di autorizzazione definiti a livello del sistema operativo e a livello applicativo.
D	Controllo integrità dei dati	Sono attivi servizi di controllo per presenza di virus nei file systems locali dei singoli PC oltre che sui messaggi di posta elettronica la cui policy di sicurezza è demandata al fornitore (Google).
E	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).

F	Gestione delle politiche di sicurezza	Sono predisposte delle Policy IT indirizzate alla sicurezza; tracciabilità delle operazioni svolte da ciascun dipendente; adozione di procedure aziendali e provvedimenti disciplinari.
G	Supporti rimovibili	Sono disposte regole per la gestione di supporti rimovibili in presenza di dati sensibili.
H	Procedure automatiche di cancellazione dati utenti interni	Ci sono regole di cancellazione dei dati in relazione alle diverse attività svolte.
I	Misure di sicurezza implementate per il servizio IT	Sono predisposte delle Policy IT indirizzate alla sicurezza per accesso ai data center.
J	Formazione degli incaricati	E' previsto un piano di formazione e di aggiornamento sulla disciplina prevista dal Codice Privacy per gli incaricati di Zucchetti Software Giuridico.

Classificazione e scheda dettagliata delle Misure di sicurezza adottate

CLASSE MISURA	MISURA	DESCRIZIONE SINTETICA
A	A.1 Accesso ai locali	L'accesso è suddiviso in tre livelli: -il primo necessita di una chiave speciale consegnata ai capi reparto; -il secondo consiste in una porta tagliafuoco munita di serratura yale la cui chiave è stata assegnata solo ad alcuni dipendenti; -il terzo viene consentito tramite identificazione effettuata a mezzo tesserino RFID personale (Badge) assegnato ad ogni dipendente. L'accesso di terzo livello è possibile solo nelle fasce orarie di svolgimento dell'attività d'ufficio e solo se l'accesso di primo e secondo livello è stato sbloccato. Qualora dovessero esserci delle esigenze particolari il lavoratore può chiedere al titolare la chiave speciale di primo accesso. Le autorizzazioni di accesso alle sedi sono fornite dall'Ufficio del personale che abilita in funzione della mansione svolta o delle esigenze segnalate.
	A.2 Registrazione accessi agli uffici	Data ed ora di ingresso ed uscita del personale impiegatizio vengono registrati tramite l'ausilio di apparecchi di rilevazione presenze.
	A.3 Prevenzione incendi	I locali sono dotati di impianti automatici di rilevazione fumo. I locali tecnici prevedono un impianto per lo spegnimento degli incendi. Sono applicate le misure di sicurezza previste dal Dlgs 81/2008.
	A.4 Dislocazione degli apparati attivi e dei server di rete	Tutti gli apparati attivi ed i server di rete sono dislocati in locali tecnici ad accesso controllato.
B	B.1 Adozione di procedure di gestione delle credenziali di autenticazione	Ogni dipendente può accedere alla propria postazione e alle infrastrutture condivise (NAS) solo attraverso il superamento di procedure di autenticazione che prevedono l'utilizzo di credenziali di accesso nominali associate agli incaricati. Un' ulteriore autenticazione permette all'utente di accedere alla propria posta

		elettronica la cui policy di sicurezza del dato è demandata al fornitore (Google). Ogni utente è dotato poi di ulteriori credenziali nominali per l'accesso all'interfaccia amministrativa dell'applicativo Fallco web. Il processo di autenticazione avviene obbligatoriamente tramite il canale https. Tutti i lavoratori sono identificati nel sistema informativo attraverso una User name, assegnata in modo univoco agli stessi, e una password. La User name non sarà associata ad altri lavoratori neppure in tempi diversi. Essa si compone di "nome.cognome". Ogni sistema ha la propria gestione e memorizzazione della User name. La password al primo accesso viene impostata dal servizio IT che configura inizialmente l'ambiente di lavoro di ogni singolo incaricato; quest'ultimo al primo accesso viene obbligato a cambiare la password. Ogni utente che inizia un trattamento di dati personali viene edotto sull'importanza che la componente riservata della credenziale di autenticazione non venga divulgata ad altri operatori. L'incaricato viene formato sulle regole minime di composizione delle password (almeno 8 caratteri e costituita da caratteri alfanumerici) e viene inoltre edotto sulla necessità di modifica di tutte le password ogni sei mesi. Questi adempimenti sono a carico dello stesso utente che assume tale onere con la sottoscrizione della lettera di incarico. Le password di tutti i sistemi elettronici quando vengono digitate sono in formato inintelligibile, cioè riportano asterischi e non caratteri alfanumerici.
	B.2 Uso esclusivo delle credenziali di autenticazione	Ogni credenziale di autenticazione (username e password) viene assegnata ad un unico operatore che la utilizzerà in modo esclusivo.
	B.3 Disattivazione delle credenziali di autenticazione per perdita qualità	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) le credenziali al medesimo riferite saranno disattivate e non verranno più utilizzate. La casella di posta elettronica dell'utente verrà chiusa contestualmente alla cessazione del relativo rapporto di lavoro.
	B.4 Verifica delle credenziali	Tutte le credenziali sono verificate con cadenza annuale al fine di controllarne l'effettiva corrispondenza con le mansioni effettivamente svolte.
	B.5 Divieto di lasciare incustodita la postazione di lavoro durante una sessione di trattamento.	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: * prolungata assenza o impedimento dell'incaricato; * l'intervento è indispensabile ed indifferibile; *presenza di concrete necessità di operatività e sicurezza del sistema. Qualora l'incaricato dovesse avere la necessità di allontanarsi dalla propria postazione lavorativa, tutti gli strumenti elettronici sono comunque dotati di sistema di blocco automatico a tempo con obbligo di reintrodurre la password per l'accesso.

C	C.1 Profilo di autorizzazione per singolo incaricato	I sistemi di Fallco web e Fallco aste hanno accessi che vengono definiti a livello applicativo in base al ruolo dell'utente connesso. 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 a stabilire a quali aree del sistema informatico l'incaricato possa accedere e quali azioni, una volta entrato, possa compiere.
	C.2 Aggiornamento periodico dei profili di autorizzazione	Ad ogni incaricato, prima di iniziare il trattamento, viene configurato un profilo di autorizzazione. Il profilo di autorizzazione viene configurato dal responsabile dell'area 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 responsabile dell'area inviando una email scritta al responsabile del servizio IT che provvede ad implementare i livelli di autorizzazione. Se in corso di rapporto di lavoro viene valutata l'esigenza di estendere o restringere il profilo di autorizzazione, sarà il responsabile dell'area ad inviare la comunicazione al servizio IT al fine di provvedere a tale adempimento.
D	D.1 Architettura sicurezza informatica	Ogni PC ha un sistema software di firewall, antivirus e anti malware con aggiornamento automatico più volte al giorno. Tale sistema effettua una scansione automatica del PC con cadenza giornaliera e ha una configurazione sempre attiva che va a monitorare accessi anomali. I sistemi operativi installati sui PC vengono aggiornati forzatamente appena il produttore rilascia aggiornamenti. La policy aziendale prevede la dismissione di sistemi operativi non più supportati dal produttore (rilasci di patch di sicurezza). Oltre al sistema firewall locale dei singoli PC, è previsto anche un sistema di firewall di rete aziendale aggiornato con cadenza mensile.
E	E.1 Procedure di backup	Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera. Il servizio di backup è sviluppato in Zucchetti Software Giuridico. Un backup completo avviene con cadenza giornaliera; un secondo tipo di backup avviene in modo selettivo con storico di 14 giorni.
	E.2 Alta affidabilità	Il file system condiviso ha un sistema RAID che assicura il corretto funzionamento anche in caso di rottura di un disco. Sono previste 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.

F	F.1 Policy per l'utilizzo degli strumenti IT	Sono predisposte policy per l'utilizzo degli strumenti elettronici relativamente agli aspetti di: ● Utilizzo del Pc ● Navigazione internet ● Utilizzo della posta elettronica La responsabilità di gestione delle stesse è affidata al servizio IT. I dipendenti sono tenuti a firmare un accordo di riservatezza prima di iniziare il rapporto lavorativo. Le procedure sanzionatorie applicabili in caso di mancato rispetto delle policy per l'utilizzo degli strumenti elettronici sono previste dal CCNL e sono rese pubbliche nel portale HR.
G	G.1 Supporti rimovibili	Nel caso di trattamento di dati sensibili o giudiziari o che presentano rischi specifici si è data la regola che non è permesso salvare detti dati su supporti rimovibili; nel caso vi sia comprovata necessità di esportare tali dati, i supporti dovranno essere crittografati.
	G.2 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.
	G.3 Riutilizzo supporti rimovibili	I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o possono essere riutilizzati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
H	H.1 Procedure di cancellazione dei dati	Sono predisposte procedure di cancellazione dei dati nei seguenti casi: ● 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 inviato al servizio IT al fine di valutarne la reale cessazione del ciclo di vita. Se l'addetto del servizio IT valuta che lo strumento elettronico deve essere dismesso, prima di consegnarlo allo smaltitore o all'acquirente esterno, formatta i dischi di memoria; i supporti rimovibili e non, quando cessano il loro ciclo di vita, vengono fisicamente distrutti.

I	I.1 misure di sicurezza implementate per il servizio IT	L'accesso alle singole risorse dei datacenter Zucchetti Spa di Lodi (Database, storage, server) e del datacenter Amazon AWS (Database, storage, server) viene definito con granularità dal responsabile dell'area IT a seconda dell'ambito e del livello del tecnico. I servizi di Amazon AWS vengono amministrati tramite un apposito pannello, raggiungibile tramite connessione sicura HTTPS e credenziali nominali assegnate ad ogni tecnico coinvolto e ogni connessione viene loggata ed il log viene mantenuto per un anno. Ogni connessione al datacenter Zucchetti Spa avviene tramite un collegamento VPN diretto utilizzando credenziali nominali che vengono aggiornate obbligatoriamente ogni sei mesi. Ogni connessione viene loggata ed il log mantenuto per un anno. I diritti di amministrazione dei sistemi nel datacenter sono demandate completamente al personale tecnico del Datacenter Zucchetti SpA.
J	J.1 Formazione degli incaricati	Sono previste istruzioni specifiche per tutti i lavoratori per il trattamento dei dati personali. Queste istruzioni vengono date attraverso la divulgazione di un'Infografica distribuita a tutti i lavoratori con una mail. Nell'infografica sono inseriti dei collegamenti ipertestuali che collegano le novità normative con le procedure operative interne a tutela dei dati personali. All'infografica segue poi una sessione formativa. Le procedure sanzionatorie applicabili in caso di mancato rispetto delle istruzioni oggetto di formazione sono previste dal CCNL e sono rese pubbliche nel portale HR.

4. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS e 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 removibili 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

CLASSE MISURA	MISURA	DESCRIZIONE SINTETICA
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
	1.2 Accesso alle postazioni di lavoro e agli archivi correnti e permanenti in formato cartaceo (sistema Badge)	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. 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. L'identificazione del lavoratore che accede alla sede avverrà anche in questo caso attraverso la rilevazione dell'apertura della porta.
	1.3 Controllo Accessi Aree Riservate	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.
	1.4 Prevenzione incendi	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.
	1.5 Dislocazione degli apparati attivi e dei server di rete	Tutti gli apparati attivi ed i server di rete sono dislocati in locali tecnici ad accesso controllato.
	1.6 Registrazione accessi agli uffici	Data ed ora di ingresso ed uscita del personale impiegatizio vengono registrati tramite l'ausilio di apparecchi di rilevazione presenze.

	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	Tutti i lavoratori sono identificati nel sistema informativo attraverso una user name assegnata in modo univoco agli stessi. 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. Le username si suddividono in username per accesso ad ambienti di lavoro e username per accesso alle applicazioni funzionali. 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.
	2.2 Adozione di procedure di gestione delle credenziali di Autenticazione: PASSWORD	L'accesso ad ogni ambiente o strumento elettronico avviene attraverso credenziali di autenticazione. 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: - 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. Ogni utente che inizia un trattamento di dati personali viene edotto sull'importanza che la componente riservata della credenziale di autenticazione non venga divulgata ad altri operatori. 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. 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). 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. Le password di tutti i sistemi elettronici quando vengono digitate sono in formato inintelligibile, cioè riportano asterischi e non caratteri alfanumerici.
	2.3 Uso esclusivo delle credenziali di autenticazione.	Ogni credenziale di autenticazione (username e password) viene assegnata ad un unico operatore che la utilizzerà in modo esclusivo.

	2.4 Disattivazione delle credenziali di autenticazione per mancato utilizzo (+ 6 mesi) o perdita qualità	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: Immediatamente, nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere allo 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); In ogni caso, entro sei mesi di mancato utilizzo.
	2.5 Verifica delle credenziali	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. C'è un firewall che limita e identifica gli attacchi e genera delle blacklist
	2.6 Divieto di lasciare incustodita la postazione di lavoro durante una sessione di trattamento.	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: * prolungata assenza o impedimento dell'incaricato; * l'intervento è indispensabile ed indifferibile; * presenza di concrete necessità di operatività e sicurezza del sistema; In tal caso dell'accesso effettuato si dovrà provvedere ad informare tempestivamente l'incaricato cui appartiene la parola chiave.
M3	3.1 Profilo di autorizzazione per singolo incaricato	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.
	3.2 Aggiornamento periodico dei profili di autorizzazione	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 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.
M4	4.1 Architettura sicurezza informatica	È previsto un insieme di regole comportamentali e procedure operative dirette a proteggere l'intero sistema informatico. 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. 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. 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. Gli stessi devono svolgere almeno le seguenti funzioni: * 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. È 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 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.
M5	5.1 Procedure di backup	Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera. Il servizio di backup è sviluppato in DC Zucchetti. Un altro backup avviene sulla macchina server in locale; un terzo tipo di backup viene effettuato su tutte le tabelle e salvato su un server locale
	5.2 Procedure di ripristino	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. **-** I backup giornalieri del DB vengono mantenuti per 30 giorni.
M6	6.1 Policy per l'utilizzo degli strumenti IT	Sono predisposte policy per l'utilizzo degli strumenti elettronici relativamente agli aspetti di: - Utilizzo del Pc; - Navigazione internet - Utilizzo della posta elettronica La responsabilità di gestione delle stesse è affidata all'Ufficio Tecnico sezione Sicurezza.
M7	7.1 Piano di Formazione degli incaricati	È 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 dal Codice 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. È stato costituito un settore aziendale, Accademia Zucchetti, che è incaricato di evadere le richieste formative provenienti dai diversi settori o divisioni di gruppo.
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	Ci sono procedure automatiche di cancellazione dei dati nei seguenti casi: ● 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 all'acquirente esterno, formatta i dischi di memoria. ● Distruzione supporti rimovibili: i supporti rimovibili quando cessano il loro ciclo di vita vengono fisicamente distrutti.
M10	10.1 Backup	Qualora la base dati è crittografata anche i backup sono crittografati. È implementato un sistema di cifratura dei backup dei servizi di DC

5. 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 Codice 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 GDPR (Reg. 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. È 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 estinguente 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.

- Outing: 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 sarin …). 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 sono erogati tramite connessione Internet protetta (https). Il cliente potrà scegliere di predisporre a propria cura e spese una linea di comunicazione VPN o MPLS.

6.MISURE DI SICUREZZA APPLICATE DA ALTRI FORNITORI

FAIV FEDERAZIONE ARTIGIANI IMPREND.
https://www.confartigianatovicenza.it/privacy-policy/

GOOGLE IRELAND LIMITED
https://gsuite.google.com/security/?secure-by-design_activeEl=data-centers
https://support.google.com/googlecloud/answer/6057301?visit_id=636779828934424041-3894545554&rd=1
https://admin.google.com/terms/apps/3/1/en/dpa_terms.html

AMAZON WEB SERVICES EMEA SARL
https://aws.amazon.com/it/security/
https://aws.amazon.com/it/legal/
https://aws.amazon.com/it/blogs/security/aws-gdpr-data-processing-addendum/

ATLASSIAN PTY LTD
https://www.atlassian.com/trust/security/security-practices#faq-5c0511ed-79a8-4e93-a9e9-437b8b8889b8
LIVESTORM
https://livestorm.co/gdpr
https://livestorm.co/privacy-policy/

MAILGUN TECHNOLOGIES
https://www.mailgun.com/privacy-policy

MICROSOFT http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46

SLACK
https://slack.com/intl/en-it/terms-of-service/data-processing