Autore	Responsabile sviluppo
Approvazione	Francesco Medda

Versione Revisione

Versione	Autore	Data emissione	Motivo della revisione
0.0	Responsabile sviluppo	01/03/2021	Prima emissione

REGISTRO DEL TRATTAMENTO
SCLOBY

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Scloby srl				
Partita Iva	10964920010				
Indirizzo	Via Luigi leonardo Colli, 3				
Città	Torino	**Cap**	10128	**PV**	TO
Legale Rappresentante	Francesco Medda				

STRUTTURA ORGANIZZATIVA			
Divisione	Direzione	Responsabile Divisione	Francesco Medda
Area	Amministrazione	Responsabile Reparto	Cristina Mainardi

INCARICATI DEL TRATTAMENTO
Sviluppo, Controllo qualità, Help desk, Commerciali, Amministrativi

DATI DI CONTATTO			
Responsabile del trattamento	Scloby Srl	amministrazione@scloby.com	0110701550
Rappresentante del titolare	N/A		

DESCRIZIONE
Scloby è una piattaforma cloud per la gestione di attività commerciali/ristorazione. Permette al commerciante di gestire, accedendo tramite browser o app ad un account riservato, tutte le proprie attività inerenti al negozio/ristorante. A titolo esemplificativo: emissione di scontrini e fatture, gestione anagrafica clienti, raccolta punti, fidelity card, gestione magazzino, ecommerce. Vengono forniti anche dei portali self-service (e-commerce) con cui il cliente finale può finalizzare gli acquisti/ordini/prenotazioni. Il sistema permette inoltre, attraverso un insieme di integrazioni ed API, di scambiare dati in modo controllato con gli altri software scelti dal commerciante.

FINALITA' DEL TRATTAMENTO
La finalità del trattamento è quella di erogare i servizi di assistenza e manutenzione al Titolare.

CATEGORIA INTERESSATI
Commercianti, Dipendenti dei commercianti, Clienti finali, Fornitori, Rivenditori

CATEGORIE DI DATI PERSONALI
Registri di accesso per ogni utente (commerciante, dipendente del commerciante, dipendente Scloby, rivenditore) Dati personali dei clienti finali e dei rivenditori, tra cui: · Nome · Cognome

· Denominazione societaria · Email/PEC · Data di nascita · Telefono · Piva/CF · Indirizzo di fatturazione · Indirizzi di spedizione/consegna · Informazioni sugli acquisti effettuati (descrizione prodotti, data/ora, metodo di pagamento) · Informazioni sulle prenotazioni effettuate (tavoli, sedute, ecc)
CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI
Subappaltatori AWS come provider del servizio di DC
TRASFERIMENTO DATI ALL'ESTERO
Non è previsto il trasferimento dei dati in Paesi Extra UE
TERMINI PER LA CANCELLAZIONE DEI DATI
I dati conservati nella Dc di AWS. Entro 30 giorni dalla cessazione del contratto, il Cliente/Titolare del trattamento potrà richiedere a Scloby copia dei dati, che la stessa fornirà in formato standard (csv). I dati stessi verranno cancellati dopo allo scadere dei 30 giorni dalla disattivazione del servizio.

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza configurabili nel sistema applicativo sono:

- *Gestione credenziali di accesso*

- User name: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Nel sistema c'è una credenziale amministrativa che viene consegnata al titolare e da questo utilizzabile sono in circostanze eccezionali. Il titolare deve predisporre una procedura organizzativa affinchè tale utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione.
- Password: le regole di complessità della password sono impostate di default all'interno del sistema; la password è configurata con le seguenti caratteristiche: alfanumerica, maiuscole e minuscole e carattere speciale.
- Il sistema prevede, dopo 10 tentativi di accesso falliti, l'attivazione della funzione CAPTCHA Block User account enumeration e il blocco temporale dell'account;
- Disattivazione/disabilitazione credenziali: anche i tempi di disattivazione delle credenziali inutilizzate o la disabilitazione delle credenziali di incaricati che non hanno più le caratteristiche soggettive per accedere a quei dati personali sono configurabili nel sistema da parte del titolare.
- Il sistema è configurabile con un sistema SSO attraverso un token.

- *Minimizzazione:*

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

- *Identificazione di chi ha trattato i dati:*

- Strumenti di log: Il Titolare può attivare i log della procedura con cui sono registrati gli accessi alla procedura stessa e alle singole funzioni che la compongono con il tipo di operazione eseguita. In particolare, è possibile attivare i log di verifica e controllo di ogni tabella applicativa (tra cui attività di inserimento, modifica e cancellazione). E' il Titolare che deve scegliere quali tabelle monitorare.

Il log dovrà essere estratto dal titolare e viene conservato nel sistema per 45 giorni.

- Presenza di utenze di servizio per personale di assistenza: Coloro che eseguono assistenza e manutenzione sulla procedura hanno utenze nominali che dovranno essere attivate e disattivate dal Titolare in funzione della necessità.

- *Tecniche di crittografia:*

- Crittografia delle password: viene registrato un hash delle password con l'algoritmo sha512 aggiungendo un "salt".*Privacy by default*
- Attivazione profilo utente: gli utenti nel portale 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 dovrà inviare una richiesta di assistenza al fornitore, che in accordo con lo stesso, procederà alla cancellazione dei dati richiesti.
- Per garantire il diritto dell'interessato di avere informazione su quali dati tratta il Titolare e alla portabilità dei suoi dati, all'interno di Scloby c'è la possibilità di fare delle estrazioni CSV dei dati.

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 accedono presso la struttura del Titolare per fare formazione od effettuare attività tecnica di manutenzione.
In questo caso gli addetti Scloby lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezze implementate dallo stesso. I Titolari potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere in affiancamento per formare il loro personale.
Qualora durante l'attività di assistenza l'addetto Scloby abbia la necessità di prelevare archivi o db di cui necessita per risolvere le problematiche evidenziate è necessario che informi il Titolari e registri tale attività sulla Nota di intervento:
Al termine dell'attività presso gli uffici Zucchetti sarà informato il Titolari sulla soluzione adottata e sulla successiva cancellazione dell'archivio.
Qualora vi fosse la necessità di conservare gli archivi per il tempo necessario al collaudo della soluzione adottata, dovrà essere informato il Titolare sul tempo massimo di conservazione di tali archivi.

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB/WHATSAPP

Nell'assistenza tramite email i tecnici Scloby inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.
L'addetto Scloby non è autorizzato a farsi mandare le credenziali di accesso del Titolare via email/form/whatsapp né tantomeno potrà salvarle sullo strumento di ticketing.
Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico Scloby è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico Scloby dovrà accedere con le proprie credenziali di assistenza oppure collegamento tramite Team Viewer (o altro strumento di teleassistenza).
I tecnici Zucchetti firmeranno ogni email con nome e cognome e l'informazione sarà salvata nel ticketing.

ASSISTENZA ATTRAVERSO LA RICEZIONE DI DATA BASE DEI CLIENTI

Qualora per risolvere il problema segnalato dal Titolare fosse necessario farsi mandare la base dati o altri files o query contenenti dati personali è necessario comunicare al Titolare o l'area ftp/sftp/ftps su cui dovrà caricare i file oppure per i Titolari con l'ambiente installato sul ns. data center, richiedere l'autorizzazione per far effettuare la copia ai nostri sistemisti.

Area FTP/SFTP/FTPS

L'area ftp sarà impostata affinché il Titolare veda solo l'upload. Il download sarà visualizzato solo dal gruppo di assistenza a cui la richiesta di assistenza è stata effettuata.

Scaricamento archivi tramite wetransfer/dropbox/gdrive o link di collegamento su ambienti del Titolare

In questo caso la gestione è in carico al Titolare che fornirà le credenziali per accedere all'ambiente dove risiedono gli archivi.
L'assistenza dovrà scaricarli in dischi di rete non soggetti a backup e cancellarli al termine dell'attività come nelle altre ipotesi.

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

Qualora i dati personali del Titolare siano sul DC di AWS in nessun caso l'assistenza di 1 livello potrà richiedere il backup ai sistemisti di Data center se non previa autorizzazione del Titolare stesso.
I sistemisti non potranno estrarre nessun backup dei Titolari per esigenze e finalità differenti rispetto al fornire assistenza agli stessi; ad esempio non potranno essere effettuati backup indirizzati alla produzione per l'esecuzione di test.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO TEAM VIEWER

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

- Il collegamento è sempre richiesto dal Titolare
- Le credenziali di accesso sono sempre individuali
- Il Titolare fa accedere i tecnici Scloby ad un ambiente con profilo di autorizzazione da lui scelto per far eseguire le attività di assistenza
- Il Titolare può disconnettere il tecnico quando desidera

Attraverso Team Viewer è possibile far accedere anche l'assistenza di 2 livello alla stessa sessione aperta. In questo caso il Titolare ne ha l'evidenza perché fornita dallo strumento e quindi accetta implicitamente tale modalità
È essenziale utilizzare il Team Viewer Scloby 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

Qualora si verifichino le seguenti casistiche:

- Conversione o start up con contratto
- Conversioni o startup senza contratto

Nel primo caso le attività sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite.
In questo caso è necessario redigere un documento di progetto in cui si convengono con il Titolare le modalità operative di esecuzione delle attività tra cui:

- Dati personali, archivi, base dati di cui necessita l'esecuzione delle attività
- Dettaglio delle operazioni da eseguire sui dati
- Identificazione del periodo entro cui sarà terminata tale attività
- La previsione di un collaudo in cui il Titolare proverà la conversione

I documenti che il Titolare ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Scloby di svolgere tutte le attività necessarie all'erogazione del servizio.
In questo caso non serve mandare al Titolare la lettera di incarico, in quanto la stessa viene fatta da Scloby, in qualità di responsabile, agli addetti Scloby .
Qualora non vi sia il contratto invece è necessario inviare al Titolare la nomina a responsabile al trattamento.
Nella nomina dovrà essere previsto un termine di svolgimento e portata a termine dell'attività. Scloby provvederà ad incaricare gli addetti in qualità di responsabile.
Anche in questo caso è necessario prevedere una fase progettuale in cui condividere gli step sopra riportati.
Al termine sarà anche in questo caso essenziale prevedere il collaudo.
Con il documento di collaudo, che dovrà essere sottoscritto dal Titolare, lo stesso ci dichiarerà che le attività da noi 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 Titolare ha provato la conversione e dichiara che il prodotto funziona e tutte le funzioni sono state correttamente configurate e implementate
- Che non ci sono errori nei dati convertiti e che quindi potrà utilizzare il prodotto per le finalità per cui lo ha acquistato

Inoltre il Titolare deve dichiarare che dalla data della firma del contratto non avrà nulla a pretendere rispetto all'attività di conversione svolta e prevista dal contratto e che autorizza Scloby a cancellare ogni dato, archivio, data base che è servito per portare a termine la fase di conversione.
Solo qualora ci fosse la necessità di mantenere gli archivi del Titolare per finalità di cautela e verifica del lavoro da noi svolto, dobbiamo inviare una comunicazione con la quale il Titolare ci autorizza a conservare gli archivi per l'ulteriore periodo, terminato il quale gli archivi dovranno essere eliminati.
Tutto l'iter autorizzativo dovrà essere inserito nel post vendita al fine di averne memoria.

Tutti i documenti contenenti dati dei Titolari stampati non possono essere riutilizzati come carta da riciclo e devono essere immediatamente distrutti.

3. MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS e AL DATA CENTER

Il datacenter scelto da Scloby implementa le seguenti misure di sicurezza
Ispezione della rete progettata per rilevare e proteggere i carichi di lavoro da traffico dannoso o non autorizzato.
Procedure automatica di rilevamento e protezione da malware e altre minacce rilevate sul sistema operativo o sull'host. Include AV, EDR, EPP, FIM e HIDS.
Registrazione centralizzata, creazione di report e analisi dei log per fornire visibilità e approfondimenti sulla sicurezza.
Controllo degli accessi e dell'identità di ogni addetto Scloby
Protezione da attacchi DDoS

Il personale Scloby è dotato di credenziali di accesso nominative e two step authentication. L'accesso alle macchine database è nettamente separato dalle macchine computazionali. Solo il personale che si occupa della mantainance dei database può accedere agli stessi.

l servizio Saas viene erogato dai sistemi Cloud di Amazon Web Services (AWS), le cui sicurezze sono consultabili ai seguenti link:
https://aws.amazon.com/it/compliance/gdpr-center/
https://aws.amazon.com/it/security/