



Autore	Ufficio privacy
Approvazione	Pietro Giordano

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio privacy	24/03/2022	25/03/2022	Prima emissione
1.0	Ufficio Privacy	15/01/2024	15/01/2024	Aggiornamento Approvatore

PARERE DPO Ok

**CORSO “ESPERTO IN CRISI D’IMPRESA “**

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	Divisione HR	Responsabile Divisione	Uggeri Domenico		
Area	Area Piattaforma Base HR & Tools	Responsabile Reparto	Alberto Cazzulani		
INCARICATI DEL TRATTAMENTO					
Addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti					
DATI DI CONTATTO					
Responsabile 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					
Il servizio erogato prevede la messa a disposizione di contenuti formativi e/o corsi di formazione fruibili mediante la piattaforma KAJABI, ossia una piattaforma LMS (Learning Management System) che eroga contenuti formativi su Web, in modalità asincrona, verso gli utenti che dispongono di un account. Corso di 55 ore - pre registrato - valido per l'iscrizione all'elenco degli Esperti ai sensi del D.L. 118/2021 e del Decreto Min. Giustizia del 28/9/2021.					
FINALITA' DEL TRATTAMENTO					
La finalità del trattamento è quella di erogare i servizi formativi, di assistenza e manutenzione al Titolare.					
CATEGORIA INTERESSATI					
Utenti della piattaforma Kajabi					
CATEGORIE DI DATI PERSONALI					
Nome, Cognome, E-mail, Username					
CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI					
Aziende del gruppo Zucchetti MyGo come erogatore del Corso					



Kajabi come provider della piattaforma
TRASFERIMENTO DATI ALL'ESTERO
No
TERMINI PER LA CANCELLAZIONE DEI DATI
Kajabi conserverà i Dati del Cliente fino al completamento del corso e non più di 2 anni dall'attivazione.



DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEL 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. Lo username può corrispondere all'indirizzo e-mail dell'utente. Il titolare deve predisporre una procedura organizzativa affinché tale utenza sia assegnata ad un unico incaricato e sia gestita in conformità alle buone regole di gestione.
- Password: 8 caratteri alfanumerici e scadenza ogni 6 mesi. Per accedere la prima volta alla piattaforma, ogni utente dovrà seguire un link univoco contenuto in una mail di invito all'esperienza formativa: questo link consentirà all'utente di impostare una propria password.
- *Tecniche di crittografia:*
- Kajabi crittografa i dati in transito utilizzando sicuri protocolli crittografici SSL/TLS.
- *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 tramite piattaforma. Qualora il Titolare decida che i dati debbano essere cancellati non sarà più reperibile alcuna informazione neppure indiretta su quell'interessato. Nei singoli applicativi saranno presenti quindi solo informazioni anonime non riconducibili neppure indirettamente ad alcun interessato. Le funzioni di cancellazione avvengono per anagrafica soggetto.

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



2. MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

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 i tecnici 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 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 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 dovrà richiedere credenziali individuali oppure collegamento tramite Team Viewer.

I tecnici firmeranno ogni email con nome e cognome e l'informazione sarà salvata nel ticketing.

Scaricamento archivi tramite wetransfer 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.



3. MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI DATA CENTER

LOCALIZZAZIONE FISICA DEI DATI

I sistemi informativi e l'infrastruttura tecnica di Kajabi sono ospitati all'interno data center di livello mondiale, accreditati SOC 2 dai nostri partner di hosting. I controlli fisici di sicurezza presso i nostri data center includono monitoraggio 24x7, telecamere, visitatori registrati, requisiti di accesso e gabbie dedicate per l'hardware Kajabi.

TERZE PARTI E SUB-RESPONSABILI DEL TRATTAMENTO

Kajabi si avvale di terze parti per fornire i nostri servizi. Esaminiamo la nostra terza parte fornitori di servizi su base regolare per garantire che stiano impiegando l'industria migliori pratiche nel loro approccio alla sicurezza e alla protezione dei dati. In termini di integrazioni fornite ai clienti, Kajabi lavora per integrarsi solo con terzi parti che si allineano alle migliori pratiche di sicurezza e privacy.

ACCESS CONTROL

L'accesso alle risorse tecnologiche di Kajabi è consentito solo in modalità sicura connettività. La nostra politica sulle password di produzione segue le migliori pratiche come indicato da autorità come il NIST. Kajabi concede l'accesso in base al principio del privilegio minimo, esamina regolarmente le autorizzazioni e revoca l'accesso immediatamente dopo il dipendente cessazione o separazione. Kajabi garantisce che l'accesso ai dati degli utenti sia limitato a responsabilità aziendali o basate su attività (ad es. Risorse umane è l'unico team con accesso ai dati HR).

COMUNICAZIONE CIFRATA

Criptiamo i tuoi dati in transito utilizzando protocolli crittografici TLS sicuri. I dati sono crittografato a riposo ove possibile.

SVILUPPO DELL'INFRASTRUTTURA

Il nostro team di sviluppo utilizza tecniche di codifica sicure e best practices, incentrato sulla Top Ten di OWASP. Gli sviluppatori sono formati sul Web sicuro per pratiche di sviluppo delle applicazioni regolarmente. Gli ambienti di sviluppo, test e produzione sono separati. Tutti i cambiamenti sono sottoposti a revisione paritaria e registrati a fini di prestazioni, audit e forensi in precedenza alla distribuzione nell'ambiente di produzione.

AGGIORNAMENTI DI SICUREZZA E AUDIT

Kajabi mantiene politiche e procedure di risposta agli incidenti di sicurezza che coprono il risposta iniziale, indagine, notifica al cliente (non meno di quanto richiesto da legge applicabile), comunicazione pubblica e risanamento. Queste politiche sono revisionato regolarmente e testato almeno ogni due anni.

Kajabi garantisce che tutti i backup vengano regolarmente analizzati per il corretto ripristino mantenere la disponibilità. I backup vengono archiviati nell'ambiente di produzione in preservarne la riservatezza e l'integrità.



Allegato 1

DATI OGGETTO DI RESTITUZIONE ALLA CESSAZIONE DEL CONTRATTO

1) Contacts.csv

Riassunto della situazione di ogni utente a livello generale.

La tabella Database di riferimento per l'estrapolazione dei dati è la tabella *"users"*, salvo diversamente indicato. Questi i campi principali:

- numero di attività formative disponibili all'utente;
- numero di attività formative completate dall'utente;
- ultima data di accesso in piattaforma;
- numero di attività formative completate dall'utente;
 - ultima attività svolta dall'utente;
 - livello di progresso dei vari prodotti;
- tutte le informazioni anagrafiche utili ad identificare l'utente, tra cui il suo "ID" in piattaforma e l'ID/Matricola aziendale, data creazione user;
- i principali indicatori di punteggio ottenuti dall'utente.

2) Extract-results.csv

Riassunto della situazione per ogni utente per ogni attività formativa a lui assegnata.

La tabella Database di riferimento per l'estrapolazione dei dati è la tabella *"results"*, salvo diversamente indicato. Questi i campi principali:

- *user_id*: identificativo interno alla piattaforma;
- codice parlante identificativo dell'attività formativa;
- titolo dell'attività formativa;
- data di prima pubblicazione dell'attività formativa per l'utente;
- data di primo completamento dell'attività formativa;
- data di primo accesso al LO;
- status dei risultati: percentuale di completamento;
- voto della valutazione finale data dall'utente al corso (nota: potrebbe non esserci);

3) Attestato

Attestato standard inviato a conclusione delle ore di corso obbligatorie e, se necessario, al superamento del test finale. Invio tramite automazione.