TERMINI DI SERVIZIO

Posizione geografica

Tutti i dati gestiti dai nostri sistemi, compresi i backup, si trovano in territorio europeo (attualmente in Italia, Germania, Irlanda), pertanto, sottostanno alle normative vigenti in tali aree.

Inventario dei dati

L'erogazione dei nostri servizi con l'approccio SaaS ci porta a gestire le seguenti informazioni:

- Dati dei clienti del servizio:
  - Nome, Cognome, e-mail, username di ogni utente
  - Dati relativi al comune e alle sedute consiliari
  - Video e trascrizioni delle sedute e degli eventi comunali
  - Configurazioni dei dispositivi utilizzati durante le sedute consiliari
  - Foto, gruppi politici e ruoli di personalità pubbliche che svolgono mansioni all'interno del Comune cliente
- Dati derivati dal servizio cloud
  - Revisioni delle trascrizioni di eventi comunali
  - Risultati di votazioni e relativi report
  - Risultati di appelli effettuati durante eventi comunali
  - Elenco di tutti gli eventi significativi avvenuti durante un consiglio comunale

Tutte le informazioni elencate in precedenza sono memorizzate in territorio europeo, le informazioni più sensibili sono criptate.

Registrazione e cancellazione delle utenze

I nostri servizi SaaS Civicam e App Gestione consiglio non prevedono automatismi per la registrazione o la cancellazione di nuove utenze, pertanto, l'accesso alle aree riservate del sito e la manipolazione dei dati è subordinata alla creazione di utenze da parte di membri della nostra azienda. Di seguito le procedure da svolgere per la creazione e la cancellazione di utenze:

- REGISTRAZIONE: Il cliente ci comunica l'elenco di tutti gli utenti (nome, cognome, eventuale foto, ruolo ed e-mail) che dovranno utilizzare la piattaforma. Un nostro operatore provvede all'inserimento dei dati nel nostro sistema. In seguito, vengono inviate e-mail di primo accesso per far impostare all'utente la password che preferisce. Ogni volta che si rende necessario modificare dei ruoli o aggiungere nuove utenze occorre contattare l'azienda.
- CANCELLAZIONE: Se un cliente comunica la volontà di cancellare un'utenza procediamo con la cancellazione manuale dell'utente e delle credenziali a lui associate.

Crittografia

Tutti i dati sensibili derivanti da interazioni con i nostri servizi sono protetti da crittografia in transito con protocollo TLS 1.2 e chiavi a 2048 bit o migliori. App gestione consiglio utilizza varie tecnologie per la crittografia dei dati sensibili a riposo utilizzando algoritmi AES-256. Le informazioni delle password degli utenti sono memorizzate con hashing seguendo le best practice attuali.

Smaltimento o riutilizzo sicuro delle apparecchiature

L'azienda utilizza i servizi cloud di AWS e di Aruba per tutta l'infrastruttura; pertanto, si rimanda alle politiche di servizio definite dai fornitori citati. Tali politiche sono sottoposte a controllo periodico, in quanto le aziende citate sono certificate secondo gli standard 27001, 27017 e 27018.

In caso di cessazione del contratto di fornitura con un cliente quest'ultimo ha 60 giorni di tempo per richiedere una copia dei suoi dati. Le modalità di esportazione dei dati vengono concordate al momento della richiesta. Al termine di tale periodo tutti i dati associati al cliente verranno cancellati senza possibilità di ripristino. Le informazioni di backup presenti in entrambe le infrastrutture non sono immediatamente eliminate in caso di cessazione del rapporto ma si attende la scadenza della copia per la cancellazione automatica dei backup.

Gestione delle modifiche

Per gestire l'introduzione di modifiche alle nostre funzionalità o la risoluzione di eventuali bug seguiamo un processo che ci permette di tener traccia di tutte le modifiche che vengono effettuate, sia da un punto di vista funzionale che del codice scritto (utilizzo di versioning).

In concomitanza con i rilasci più significativi vengono inviate al cliente e-mail contenenti le principali modifiche che verranno apportate al sistema ed eventuali criticità riscontrabili. Il rilascio delle modifiche viene effettuato in finestre temporali in cui i nostri servizi non sono utilizzati.

Backup delle informazioni

I dati dei clienti sono memorizzati in modo ridondante su server distribuiti in più datacenter geografici per garantire l'alta disponibilità e la resilienza dei dati. Eseguiamo backup automatici regolari dei dati, con una frequenza giornaliera e conserviamo questi backup per un periodo di minimo quattro settimane. Tutti i nostri backup in transito e a riposo sono protetti utilizzando algoritmi avanzati (AES-256) e solo il personale autorizzato può accedervi. In caso di disaster recovery utilizziamo una finestra temporale di quattro ore per ripristinare i dati. Con cadenza periodica i backup dei dati vengono verificati per confermare l'integrità dei dati. L'utente finale non può accedere ai dati di backup. Le operazioni di ripristino e di disaster recovery sono a carico dell'azienda.

Registrazione degli eventi

I nostri applicativi producono degli eventi che vengono memorizzati a intervallo variabile (minimo una settimana) per ricostruire eventuali dinamiche di errori o per identificare inefficienze dei sistemi. Con cadenza periodica vengono esaminati i log dei nostri sistemi per applicare azioni correttive in caso di identificazione di possibili miglioramenti. I nostri utenti non hanno accesso diretto a tali registri ma è possibile richiedere conferma di eventi problematici inviando una mail a assistenza@civicam.it.

Gestione delle vulnerabilità tecniche

Lato infrastrutturale ci affidiamo a partner certificati che hanno le capacità di gestire le vulnerabilità tecniche secondo la best practice attualmente conosciuta.

Lato applicativi SaaS vengono utilizzate strategie che mirano a minimizzare l'insorgere di problematiche di servizio e di sicurezza. In base al livello dell'architettura sono adottate differenti strategie.

Livello infrastrutturale - Macchine virtuali e server: Con cadenza semestrale vengono effettuati gli aggiornamenti del sistema operativo che risolvono bug. Eventuali installazioni di patch di miglioramento del sistema operativo vengono invece valutate caso per caso; ogni sei mesi viene compilato il registro che contiene le vulnerabilità tecniche, le azioni intraprese e da intraprendere.

Livello dati - database: Con cadenza semestrale vengono verificati gli aggiornamenti ai motori dei database e valutato se procedere con un aggiornamento; ogni sei mesi viene compilato il registro che contiene le vulnerabilità tecniche, le azioni intraprese e da intraprendere.

Livello applicativo – applicazioni: Ogni volta che si avvia un nuovo sviluppo viene eseguita un'analisi per il raggiungimento dell'obiettivo che tiene conto anche delle buone pratiche di sviluppo del software e della sicurezza informatica. Una volta presa la decisione il software viene sviluppato al meglio delle conoscenze e competenze informatiche del momento.

Poiché i nostri sistemi si basano anche su librerie open source di terze parti prestiamo molta attenzione alla selezione iniziale e al suo mantenimento da parte della community. In fase di selezione del pacchetto vengono valutate varie caratteristiche, le più importanti sono le seguenti:

- Attuali problemi di sicurezza della libreria
- Reputazione del pacchetto nella community di sviluppatori (stelle github, recensioni)
- Data dell'ultima modifica
- Community intorno al pacchetto (risposte alle segnalazioni, accettazione di modifiche al codice, ecc.)

Con cadenza semestrale eseguiamo per ogni singola codebase l'audit delle dipendenze che permette di identificare i pacchetti che hanno ricevuto degli aggiornamenti. In base alle nostre valutazioni decidiamo di aggiornare, pianificare o trascurare l'aggiornamento del pacchetto. In concomitanza con questo check viene compilato il registro che contiene le vulnerabilità tecniche, le azioni intraprese e da intraprendere.

Segregazione delle reti

In ambito SaaS forniamo sistemi multi-tenant dove ogni utente, previo inserimento di credenziali, può vedere o modificare le informazioni a cui è abilitato. I dati dei nostri clienti sono separati logicamente utilizzando un id univoco del portale (dominio di terzo livello) che è associato a dati e oggetti specifici dei nostri clienti. Le regole di autorizzazione sono insite nell'architettura e validate in base ai ruoli di un utente.

Analisi e specifiche dei requisiti di sicurezza delle informazioni

In quanto fornitori si sistemi Software as a Service il nostro obiettivo è di gestire la sicurezza dei dati e del servizio in generale durante tutto il suo ciclo di vita. A tal fine i controlli di sicurezza sono integrati nei processi di sviluppo e supportati dai nostri sistemi.

- Durante la fase di analisi e raccolta dei requisiti si valutano le funzionalità da aggiungere o modificare e i relativi rischi che le attività comportano.
- Nella fase implementativa vengono adottate metodologie atte a ridurre e confinare gli eventuali errori. Vengono utilizzate tecniche di sviluppo come git-flow, PR approvate da più sviluppatori, testing e pratiche di codifica sicura.
- Con cadenza periodica vengono effettuati security assessment e aggiornamenti dei componenti di terze parti
- Tutto il codice prodotto è versionato in modo da poter ripubblicare tutti i nostri sistemi in produzione in caso di disastro
- In fase di trasferimento o messa a riposo di dati si privilegia l'utilizzo di crittografia anche per dati non sensibili
- Vengono effettuati backup con cadenza giornaliera dei dati in produzione
- Per quanto riguarda il software in produzione vengono applicate patch con cadenza periodica e ogni singola modifica da aggiungere viene valutata effettuando un'analisi costi/benefici.
- Vengono memorizzati eventi in appositi registri al fine di identificare e ripercorrere eventuali problemi riscontrati
- Viene fornita formazione continua agli sviluppatori. Al personale di supporto viene fornita formazione sui principi di sicurezza.

Il nostro software è ospitato su infrastrutture di partner altamente affidabili e dotati delle principali certificazioni in ambito della sicurezza delle informazioni

Politiche di sviluppo sicuro

Lo sviluppo di nuove funzionalità e di correzione di difetti negli applicativi viene effettuato seguendo delle fasi specifiche e viene tutto tracciato tramite applicativi.

<u>Sviluppo di nuove funzionalità</u>

In caso ci fosse la necessità di aggiungere nuove funzionalità al sistema, i passaggi da svolgere sono i seguenti:

- Identificazione dei requisiti: Viene effettuata una segnalazione/proposta da un reparto dell'azienda o da un cliente e viene censita all'interno di apposito applicativo
- Pianificazione dell'attività: Quando i requisiti raccolti sono chiari viene valutato se mettere l'attività in pianificazione per procedere poi allo sviluppo software. Con cadenza mensile i ruoli preposti si riuniscono per identificare le attività da svolgere nel mese successivo.
- Sviluppo: Durante il periodo di sviluppo gli sviluppatori implementano le funzionalità descritte nell'attività seguendo l'approccio elencato in precedenza (sviluppo su rami del codice appositi, approvazione Pull Request, approvazione e pubblicazione ambiente di DEV).
- Testing: Quando la modifica del codice raggiunge l'ambiente di DEV viene testato e in caso positivo viene portato in ambiente di staging per farlo testare ai product manager. In caso di test con esito positivo l'attività viene contrassegnata come completata ed è possibile pubblicarla in produzione.
- Pubblicazione: Per minimizzare gli errori dovuti alla pubblicazione manuale delle funzionalità vengono utilizzate apposite pipeline.
- Test in produzione: Una volta completata la fase di pubblicazione vengono effettuati dei test in produzione.
- Chiusura attività: l'attività viene segnata come pubblicata.

<u>Correzione difetti negli applicativi</u>

In caso di difetto del software o altra problematica dei nostri sistemi, sia che la segnalazione sia interna che da parte di un nostro cliente, viene aperto un ticket e si procede nel seguente modo:

- Raccolta delle informazioni: Viene richiesto a chi ha individuato il difetto di fornire tutte le informazioni per poter riprodurre la problematica in oggetto. In caso il problema sia immediatamente risolvibile dall'operatore si tiene traccia del ticket e lo si chiude subito. Nel caso negativo invece viene assegnato al ruolo di riferimento per quella problematica.
- Assegnazione ticket: In base alla priorità del ticket si avvia la fase di assegnazione a una risorsa. Se il ticket è urgente va subito risolto, altrimenti viene messo a pianificazione. Nel caso di difetto software urgente si parte dal ramo di sviluppo di produzione e viene effettuata una patch del codice che viene portata in produzione non appena il problema è risolto (prima della pubblicazione vengono effettuati dei test di non regressione).
- Risoluzione del problema in produzione: Quando il problema è stato identificato e risolto la correzione viene pubblicata in produzione seguendo le stesse modalità illustrate per il paragrafo "sviluppo di nuove funzionalità".
- Test in produzione: Una volta completata la fase di pubblicazione vengono effettuati dei test in produzione.
- Chiusura ticket: il ticket viene marcato come "risolto".

Le fasi elencate in precedenza vengono svolte per migliorare la sicurezza e l'efficienza di tutto il processo di sviluppo e manutenzione degli applicativi.

Per garantire che le fasi descritte in precedenza vengano effettuate in maniera corretta sono stati creati tre ambienti distinti che corrispondono all'ambiente di DEV, STAGING e PRODUZIONE. Tali ambienti hanno le stesse funzionalità di base ma sono completamente indipendenti (sia in termini di codice che di informazioni) in modo da evitare di creare dei disservizi in caso di pubblicazione di funzionalità/bugfix da testare/implementare. Lo scopo di ogni singolo ambiente è il seguente:

- DEV: Ambiente che contiene le ultime novità in fase di sviluppo e sviluppi parziali non ancora validati dal team di sviluppo
- TEST: Ambiente che contiene nuovi sviluppi validati dal team di sviluppo, in attesa di essere validati definitivamente dai product manager
- PRODUZIONE: Ambiente che contiene tutte le funzionalità validate.

Sicurezza degli accordi

Poiché i nostri servizi sono di tipo Software as a Service il cliente può solo utilizzare l'applicativo. Non ha accesso a nessuna informazione se non quelle inerenti all'utilizzo del software. In caso di problema di natura tecnica la risoluzione spetta all'azienda che tramite accorgimenti ripristinerà il corretto funzionamento. Il cliente finale non ha quindi accesso a database e componenti dell'infrastruttura, log, codice e qualsiasi altro aspetto tecnico. I dati inseriti rimangono in possesso del cliente e saranno salvati nei nostri sistemi fintanto che sarà valido il contratto di servizio. Una volta terminato il rapporto il cliente dovrà provvedere a richiedere copia dei dati. A prescindere dalla richiesta di migrazioni dopo 60 giorni tutti i dati associati al cliente verranno cancellati. In caso di identificazione di un problema il cliente invierà una mail a assistenza@civicam.it.

Catena di approvvigionamento delle tecnologie

Tutti i nostri software sono installati su server o nodi cloud di fornitori ritenuti affidabili e in possesso delle principali certificazioni riguardanti la sicurezza delle informazioni. L'azienda non ospita alcun sistema o dato relativo ai prodotti all'interno dei propri uffici aziendali ma esternalizza l'hosting della propria infrastruttura per i prodotti a leader del settore dell'infrastruttura cloud, Amazon Web Services (AWS) e Aruba. L'infrastruttura dei prodotti si trova nei data center di AWS situati in Europa. La regione principale è situata in Irlanda e la regione secondaria è situata in Germania. Per quanto riguarda Aruba tutti i nodi si trovano in Italia. Facciamo affidamento sui programmi di sicurezza e conformità degli audit di AWS e di Aruba per l'efficacia dei loro controlli di sicurezza fisica, ambientale e infrastrutturale. AWS e Aruba garantiscono una disponibilità del servizio minima del 99%, assicurando ridondanza per tutti i servizi elettrici, di rete e HVAC. I piani di continuità aziendale e di recupero da disastri per i servizi AWS e Aruba che utilizziamo sono stati validati indipendentemente dalla certificazione ISO 27001(il fornitore AWS è in possesso di una certificazione SOC 2 Tipo 2).

Procedure di gestione degli incidenti

L'azienda ha identificato delle procedure di gestione degli incidenti e nominato un responsabile della sicurezza delle informazioni. Il cliente in caso di identificazione di problematiche di sicurezza deve comunicarlo tempestivamente all'azienda che provvederà a intraprendere attività per mitigarle. Sono state adottate soluzioni di monitoraggio e rilevamento delle minacce. L'identificazione della problematica può avvenire in due modalità:

<u>Il personale dell'azienda si accorge della problematica</u>

Una volta recepita la problematica si intraprendono le attività per mitigarla. Il cliente viene contattato e avvertito nel minor tempo possibile; in caso ci fosse necessità vengono inviate istruzioni che deve intraprendere tempestivamente al fine di limitare il danno; per comunicare la problematica l'azienda utilizzerà il telefono o l'indirizzo e-mail del responsabile dei rapporti cliente-fornitore all'interno dell'organizzazione del cliente.

<u>Il cliente si accorge della problematica</u>

Nel caso in cui è il cliente ad accorgersi della problematica questo deve comunicare tempestivamente all'azienda la problematica riscontrata utilizzando apposito canale. Al fine di mantenere sicura la gestione della problematica il cliente dovrà comunicarla solo all'azienda all'indirizzo assistenza@civicam.it.

A valle della risoluzione dell'incidente vengono svolte due attività principali:

- Analisi per miglioramento continuo: vengono analizzati i problemi e assimilate le cause. Vengono create attività all'interno del software di ticketing al fine di pianificare azioni correttive atte alla mitigazione degli effetti di tali problematiche
- Formazione: I nostri collaboratori (se di pertinenza) vengono aggiornati sulle cause dell'incidente e invitati a identificarle tempestivamente al verificarsi.

Tutta la gestione dell'incidente viene tracciato in modo da poterlo ricostruire in futuro.

Segnalazione di evento di sicurezza delle informazioni

In caso di evento di sicurezza da segnalare all'azienda sono attivi i seguenti canali di contatto:

- **E-mail:** assistenza@civicam.it
- **Telefono:** 0737787665

Il numero di telefono è attivo durante l'orario di ufficio 8:30-17:30 dal lunedì al venerdì festivi esclusi.

Raccolta delle prove

Le informazioni contenute nei registri dei nostri fornitori o in nostro possesso potranno essere utilizzate come prove per le indagini da parte delle autorità competenti.

Finalità del trattamento delle informazioni personali

L'azienda si impegna a non utilizzare le informazioni di cui viene in possesso per scopi diversi da quanto definito nel contratto.

Uso commerciale delle informazioni personali

L'azienda si impegna a utilizzare le informazioni di cui viene in possesso per scopi pubblicitari o di marketing solo previo consenso del cliente.

Trattamento delle informazioni personali in subappalto

L'azienda si avvale di subappaltatori solo per la manipolazione di contenuti e non per la gestione dell'infrastruttura cloud o degli aspetti tecnici. Tali subappaltatori sottoscrivono un contratto contenente clausole relative alla riservatezza e non divulgazione. L'azienda solitamente provvede a fornire al subappaltatore la strumentazione necessaria per lo svolgimento dell'incarico affidato, per cui sono note e attuate le misure tecniche e organizzative minime che soddisfano gli obblighi di sicurezza delle informazioni e protezione delle PII; nel caso in cui il subappaltatore utilizzi propria strumentazione, vengono stabilite contrattualmente le misure tecniche e organizzative minime da attuare di cui sopra.

Obbligo di notifica di divulgazione delle informazioni personali

In caso di richiesta da parte di un'autorità incaricata in applicazione della legge per cui l'azienda è obbligata alla divulgazione dei dati personali del cliente ne verrà data prontamente notizia al cliente tramite mail dall'indirizzo assistenza@civicam.it entro 24 ore dalla richiesta dell'autorità incaricata.

Notifica di una violazione dei dati che coinvolge le informazioni personali

L'azienda ha identificato delle procedure di gestione degli incidenti e nominato un responsabile della sicurezza delle informazioni. In caso di violazione il cliente viene contattato e avvertito nel minor tempo possibile; in caso ci fosse necessità vengono inviate istruzioni che deve intraprendere tempestivamente al fine di limitare il danno; per comunicare la problematica l'azienda utilizzerà il telefono o l'indirizzo e-mail del responsabile dei rapporti cliente-fornitore all'interno dell'organizzazione del cliente.

Identificazione della normativa applicabile e dei requisiti contrattuali

Tutti i nostri fornitori che utilizziamo per ospitare i nostri servizi si trovano in territorio europeo. In particolare utilizziamo data center che si trovano in Irlanda, Germania e Italia manutenuti da AWS e Aruba Cloud, pertanto, la normativa vigente è quella europea. Nello sviluppare le nostre funzionalità ci basiamo su leggi e regolamenti che riguardano il trattamento dei dati personali (GDPR) e le applichiamo sviluppando sistemi che applicano la crittografia sia in transito che a riposo e le migliori tecniche di sviluppo e progettazione attuali. Siamo periodicamente sottoposti ad audit da ente terzo e al termine di tali attività produciamo dei report che contengono lo stato attuale dell'azienda e le azioni migliorative da intraprendere. All'acquisizione di nuove certificazioni inviamo comunicazione ai clienti in modo da tenerli aggiornati sulle nostre conformità in merito al presente punto.

Diritti di proprietà intellettuale

Per ogni reclamo che riguarda un diritto di proprietà intellettuale inviare una mail all'indirizzo assistenza@civicam.it.

Punto di contatto in materia di informazioni personali

Il punto di contatto per quanto riguarda il trattamento delle informazioni personali è:

- **E-mail:** assistenza@civicam.it
- **Telefono:** 0737787665

Il numero di telefono è attivo durante l'orario di ufficio 8:30-17:30 dal lunedì al venerdì festivi esclusi.