

Policy in materia di protezione e disponibilità dei dati relativi ai servizi web

Premessa

Di seguito sono esplicitati termini con cui Codebase ARL tratta la materia della sicurezza informatica, continuità operativa e trattamento dei dati personali contenuti negli archivi delle scuole clienti e fruitori dei servizi Archimede

La Codebase ARL è impegnata costantemente a migliorare la qualità dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole, salvaguardando l'integrità e la riservatezza dei dati, nella continuità operativa dei servizi.

Codebase ARL adotta tutti gli accorgimenti organizzativi e le soluzioni tecniche per garantire il ripristino delle condizioni di funzionamento e di operatività antecedenti ad eventuali eventi disastrosi ed è costantemente impegnata nella ricerca di tutte le misure di sicurezza in sintonia con il quadro normativo italiano e europeo (Regolamento UE 2016/679, Linee guida AgID per il Disaster Recovery, Circolare AgID nr. 2/2017 sulle misure minime di sicurezza ICT per le PP.AA.).

Tipologia dei dati gestiti dalla Codebase ARL

I dati gestiti dalla Codebase ARL riguardano tutte le informazioni presenti negli archivi delle scuole clienti ed i dati degli utenti fruitori dei servizi web Archimede.

Nel rispetto dell'art. 9 del Regolamento UE 2016/679 , il trattamento dei dati varia in ragione della loro natura.

Possono, pertanto essere conservati informazioni personali, nel caso di servizi inerenti la gestione del personale e degli alunni o possono essere trattati dati relativi a categorie particolari (specificamente quelle riepilogate nelle schede allegate al D.M. 305/2006, recante identificazione degli ex dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione).

Architettura del sistema informatico

I database server e le copie di backup sono ospitati presso la piattaforma cloud Aruba

Il Cloud Aruba è strutturato in "regioni" , costituite da più "zone di disponibilità" ognuna delle quali è una partizione completamente isolata dell'infrastruttura, costituita da data center provvisti di alimentazione, rete e connettività ridondanti, ognuno in una propria struttura separata.

Con la loro infrastruttura di alimentazione, le zone di disponibilità sono fisicamente separate tra loro da una distanza significativa di molti chilometri.

L'amministrazione dei servizi di gestione delle applicazioni e dei database è affidata esclusivamente a personale interno alla Codebase ARL.

Gli addetti all'amministrazione delle applicazioni e dei database sono nominati amministratori di sistema.

L'accesso ai servizi di amministrazione è eseguito attraverso utenze nominative.

Con cadenza mensile viene eseguito il controllo sui log degli accessi degli amministratori di sistema da parte del personale designato.

I log degli accessi eseguiti dagli amministratori di sistema sono archiviati per un periodo di 18 mesi.

Modalità di gestione dei dati e di erogazione del servizio

Il sistema di gestione delle istanze delle applicazioni e dei database adottato da Codebase, consente di avere una facile ridondanza e replicazione dei sistemi informatici e dei dati, preservando così i clienti da rischi di interruzione prolungata dei servizi e/o di perdita delle informazioni.

Ogni cluster di database è formato da due tipi di istanze: primaria e replica.

Per ogni istanza primaria, ci sono più repliche posizionate in zone di disponibilità differenti. L'istanza database primaria viene replicata in modo sincrono.

Nel caso in cui l'istanza primaria non sia disponibile, viene eseguito automaticamente la commutazione su una replica.

Backup dei dati

Per ogni istanza di database, un servizio esegue uno snapshot giornaliero. La creazione degli snapshot non provoca alcuna interruzione delle operazioni di scrittura e lettura.

Per ciascuna istanza di database viene mantenuta una copia di backup giornaliera per 60 giorni (periodo di retention dei backup).

Durante questo periodo, è possibile eseguire il ripristino di una istanza di database a un punto temporale specifico.

Decorso questo periodo, viene mantenuta una copia settimanale.

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web archimede, è di esclusiva pertinenza della scuola.

Con l'attivazione di una nuova utenza, è richiesta l'indicazione dell'indirizzo mail, a cui saranno comunicati l'attivazione e i successivi reset password dell'utenza.

L'indirizzo email può essere modificato in qualsiasi momento dal singolo utente dalla propria area riservata.

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, la Codebase ARL esegue il tracciamento degli accessi ai servizi web e – per le applicazioni più critiche - delle operazioni effettuate dagli utenti all'interno degli stessi. I dati relativi agli accessi sono soggetti alle stesse politiche di backup dei database. I file di log delle operazioni vengono conservati per un periodo non inferiore a 6 mesi e non superiore a 24 mesi.

Per i tempi di conservazione sono possibili variazioni in ragione ed in relazione:

- a particolari esigenze tecniche o di sicurezza;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Criteri di selezione delle server farm

Ad ogni fornitore è richiesta come requisito la certificazione ISO 27001, la qualificazione come CSP presso AgID, e uno SLA di connettività di almeno il 95% su base annua e una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.

Modalità di trasmissione dei dati

I dati viaggiano sulla rete criptati, secondo il protocollo SSL che garantisce il massimo livello di sicurezza a protezione delle trasmissioni telematiche.

Disponibilità dei dati

Si fa riferimento al documento pubblicato sul sito www.registroarchimede.it
[https://www.registroarchimede.it/sites/default/files/Guida_richiesta_dati.pdf]

Risoluzione dei contratti, restituzione, cancellazione e fruibilità dei dati

In caso di risoluzione del contratto di licenza o di assistenza in essere da parte della scuola di un servizio web, il Dirigente scolastico può richiedere:

- la restituzione
- il mantenimento dei dati (a fronte di un pagamento di un canone);

- la cancellazione/anonimizzazione dei dati.

I dati vengono restituiti in formato aperto, nei tempi tecnici di esportazione sicura dei dati.

I tempi tecnici occorrenti alla cancellazione dei dati possono variare da 2 a 12 mesi, a seconda della natura dei dati interessati. L'ampiezza di tale periodo è funzionale a possibili verifiche operate dal cliente sull'operazione di migrazione dati eseguita dal nuovo fornitore.

I dati sono conservati nei sistemi di backup, al solo scopo di disaster recovery e fino allo scadere della policy di retention sopra specificata.

Impegni e garanzie per la protezione dei dati personali

Ai sensi dell'art. 28 del Regolamento UE 2016/679, la Codebase ARL garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali in outsourcing, Per la fornitura dei servizi web, la Codebase ARL assume il ruolo di Responsabile del Trattamento, previa nomina da parte del cliente. In caso di assenza di nomina formale, la Codebase ARL si riserva il diritto di sospendere l'erogazione del servizio fino ad adempimento da parte del cliente.

La Codebase ARL quale Responsabile del Trattamento dei Dati, ha il compito e la responsabilità di:

- porre in essere quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente la regolare tenuta del registro delle attività di trattamento espletate per conto dell'Istituto Scolastico.
- adottare adeguate misure di protezione dei dati personali in oggetto;
- assistere l'Istituto Scolastico per l'adempimento delle misure tecniche ed organizzative atte a garantire l'esercizio dei diritti degli interessati;

- restituire e successivamente cancellare i dati personali trattati alla cessazione del contratto, come sopra indicato, fatte salve le prescrizioni di legge;
- mettere a disposizione dell'Istituto Scolastico tutte le informazioni atte a dimostrare la conformità alla vigente normativa di fronte ad una richiesta della Autorità competente;
- comunicare senza ingiustificato ritardo qualunque avvenuta o supposta violazione di dati personali ai fini della registrazione/notifica/comunicazione dei data breach;
- provvedere immediatamente, nel caso in cui un interessato si rivolgesse alla Codebase ARL per l'esercizio di un diritto o reclamando una violazione, a comunicarlo al Responsabile della Protezione dei Dati della scuola ed all'Istituto Scolastico stesso senza rispondere all'interessato, salvo diversa istruzione della scuola;
- autorizzare il personale dedicato al trattamento dei dati, istruendolo adeguatamente e vincolandolo alla riservatezza;
- provvedere alla nomina dei concessionari in qualità di sub-responsabili del trattamento per le attività di assistenza ai software e manutenzione degli archivi dei sistemi informatici specificati nell'apposito contratto di licenza software, fornendo loro istruzioni scritte in merito alle misure di sicurezza da adottare e vincolandoli alla riservatezza dei dati.
- Vigilare costantemente sull'operato dei soggetti incaricati e dei sub-responsabili al fine di evitare che vengano disattese le misure tecniche ed organizzative atte a proteggere le informazioni personali.

Disponibilità e aggiornamento del documento

Il presente documento è disponibile sul sito Codebase ARL (www.codebase.it) all'interno della sezione "Privacy" e viene aggiornato periodicamente in base all'evoluzione dei sistemi di sicurezza adottati e delle eventuali innovazioni normative. Ad ogni aggiornamento del documento, viene data comunicazione per email a tutte le scuole clienti.