Seregno, 05 ottobre 2020

Policy di sicurezza bSmart Labs

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

Premessa

Il presente documento descrive la policy di bSmart Labs in materia di sicurezza delle informazioni, continuità operativa e trattamento dei dati personali.

bSmart Labs è impegnata costantemente a migliorare l'efficacia e l'efficienza dei propri processi di gestione delle informazioni e dei servizi web offerti alle scuole e agli utenti finali, nell'ottica della salvaguardia dell'integrità e della riservatezza dei dati, della disponibilità dei servizi e delle informazioni in tempi adeguati e della continuità operativa dei servizi e dei sistemi.

In questo contesto, bSmart Labs adotta tutti gli accorgimenti organizzativi, le soluzioni tecniche e procedurali idonee al mantenimento e ripristino delle condizioni di funzionamento e di operatività antecedenti ad eventuali eventi disastrosi ed è impegnata, con continuità, ad adottare tutte le misure di sicurezza che trovano fondamento e riferimento all'interno del 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.) e dei più elevanti standard di sicurezza delle informazioni.

Tipologia dei dati e delle informazioni gestiti da bSmart

I dati gestiti da bSmart Labs riguardano le informazioni (generiche e personali, dati personali di natura comune relativi a persone fisiche identificate o identificabili, anagrafiche e dati di contatto, identificativi dell'utente, dati statistici sul comportamento degli utenti, foto, indirizzi IP e qualunque altro dato personale di titolarità delle scuole e degli utenti finali fruitori dei servizi web bSmart.

Sede Legale: Via Montorfano 98, 20831 Seregno (MB)
Sede Operativa: Via Torino 3, 20814 Varedo (MB) - Tel. +39 0362 640018 - Fax +39 0362 642456
www.bsmartlabs.com | Email: info@bsmart.it
C.F. / P.Iva: 03728130968
Cap. Sociale Euro 10.000,00 i.v.

Modello di responsabilità condivisa

bSmart Labs lavora in qualità di fornitore di servizi in cloud mettendo a disposizione applicativi in modalità SaaS e erogando i relativi servizi di assistenza e manutenzione. Si avvale di fornitori di servizi cloud qualificati e certificati secondo la vigente normativa ed identifica nei propri contratti gli specifici ruoli attribuiti a ciascun fornitore del servizio.

Per rappresentare in maniera completa la distribuzione dei ruoli e rendere gli utilizzatori dei servizi consapevoli delle loro responsabilità nell'uso dei servizi (anche in cloud), bSmart Labs ha adottato un modello organizzativo sulla protezione dati, al fine di responsabilizzare e istruire tutto il personale autorizzato al trattamento e gestire in maniera corretta i rapporti con i fornitori esterni.

Architettura del sistema informatico

I database server e le copie di backup sono ospitati presso la piattaforma cloud AWS (Amazon Web Services). Il Cloud AWS è strutturato in "regioni", costituite da più "zone di disponibilità" (AZ), ognuna delle quali è una partizione completamente isolata dell'infrastruttura AWS, 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.

Per i dati delle scuole e dei propri utenti finali, bSmart Labs ha scelto la regione Europa Irlanda, situata nella Repubblica d'Irlanda, composta da 3 zone di disponibilità.

L'amministrazione dei servizi di gestione delle applicazioni e dei database è affidata esclusivamente a personale interno a bSmart Labs.

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 periodicità infrannuale, viene eseguito il monitoraggio sui log degli accessi degli amministratori di sistema da parte del personale all'uopo designato.

Modalità di gestione dei dati e di erogazione del servizio

bSmart Labs utilizza Amazon EKS (Kubernetes) e le istanze EC2 autoscalabili dedicate all'erogazione del servizio non contengono dati.

Il sistema di gestione delle istanze delle applicazioni e dei database adottato da bSmart Labs, 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.

Il database utilizza AWS Aurora Serverless per scalabilità, backup e failover automatici.

Backup dei dati

I dati necessari al funzionamento delle applicazioni sono memorizzati su servizio esterno Amazon EFS e salvati ogni ora su Amazon S3.

Per ogni istanza di database, il servizio AWS Aurora RDS Serveless esegue uno snapshot giornaliero e conserva i log delle modifiche al database all'interno del periodo di "retention" (v. in prosieguo). La creazione degli snapshot non provoca alcuna interruzione delle operazioni di scrittura e lettura in quanto gli "snapshot" vengono eseguiti su una copia di standby.

Per ciascuna istanza di database viene mantenuta una copia di backup giornaliera per 35 giorni (periodo di retention dei backup).

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

Gestione e Profilazione delle utenze

La gestione e profilazione delle utenze degli applicativi web bSmart Labs, attraverso il portale bSmart, è di esclusiva pertinenza della scuola o degli utilizzatori finali.

In fase di attivazione di una nuova utenza, viene richiesta l'indicazione di un indirizzo mail, a cui saranno comunicati l'attivazione e i successivi reset password dell'utenza.

L'indirizzo mail può essere modificato in qualsiasi momento dal singolo utente mediante richiesta al servizio di assistenza support@bsmart.it.

Tracciamento degli accessi ai servizi web

Ai fini della sicurezza, bSmart Labs s.r.l. esegue il tracciamento degli accessi ai servizi web bSmart 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 superiore a sei mesi.

Per le eventuali richieste dei Log da parte dei clienti, l'Azienda richiede la compilazione di apposita modulistica da inviare tramite PEC all'indirizzo bsmart@legalmail.it

Un eventuale prolungamento dei tempi di conservazione può aver luogo 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.

Oltre ai suddetti dati, i sistemi informatici e le procedure software preposte al funzionamento dei servizi web bSmart acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati e che vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso delle applicazioni e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione.

Procedure di verifica del sistema di protezione dei dati

Con cadenza annuale vengono svolte attività di Penetration test e verifiche di Vulnerability Assessment, anche attraverso test automatizzati.

Criteri di selezione delle server farm

bSmart Labs si affida esclusivamente a server farm di comprovata affidabilità ed esperienza in materia di sicurezza informatica, e comunque previa verifica delle misure fisiche, logiche e organizzative poste in capo alle infrastrutture informatiche fornite.

Ad ogni fornitore è richiesta come requisito la certificazione ISO 27001, la qualificazione come CSP presso AgID, uno SLA di connettività di almeno il 99,9% su base annua ed 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

I dati di proprietà delle scuola contenuti negli archivi della piattaforma possono essere richiesti dal parte dei Dirigenti scolastici mediante pec all'indirizzo bsmart@legalmail.it.

I dati contenuti nei database e nei repository delle applicazioni per cui è stata fatta richiesta di esportazione, sono resi disponibili per lo scarico mediante un link comunicato via PEC. L'operazione di scarico è protetta da password comunicata per email all'indirizzo indicato dal cliente nel modulo di richiesta esportazione.

Risoluzione dei contratti, restituzione, cancellazione e fruibilità dei dati

In caso di risoluzione del contratto di licenza o di assistenza da parte della scuola di un servizio, la scuola – su richiesta del Dirigente scolastico – può optare per:

- la restituzione e cancellazione/anonimizzazione dei dati (soluzione di default per legge);

- la restituzione e mantenimento dei dati (a fronte di un pagamento di un canone).

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

Dalla data di cessazione, è inoltre consentito l'accesso all'applicazione web da parte degli utenti per un ulteriore periodo di 1 mese.

I tempi tecnici occorrenti alla successiva cancellazione dei dati possono variare da 2 mesi a 12 mesi, a seconda della natura dei dati coinvolti e delle applicazioni interessate. Il periodo è peraltro funzionale ad eventuali verifiche da parte del cliente sull'operazione di migrazione dati eseguita dal nuovo fornitore.

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

Impegni e garanzie per la protezione dei dati personali

bSmart Labs garantisce che l'erogazione dei servizi avviene nel rispetto della normativa che regola il trattamento dei dati personali e, nei casi in cui effettua operazioni di trattamento in outsourcing per conto delle scuole, nel rispetto dell'art. 28 del Regolamento UE 2016/679.

Per la fornitura dei servizi web, bSmart Labs assume il ruolo di Responsabile del Trattamento, previa nomina da parte del cliente. Per la nomina a Responsabile del trattamento, già definita nelle condizioni contrattuali.

In caso di assenza di nomina formale, bSmart Labs si riserva il diritto di sospendere l'erogazione del servizio fino ad adempimento da parte del cliente, titolare del trattamento.

Responsabile per la Protezione dei Dati (DPO) della bSmart Labs, è LIQUIDLAW Srl, raggiungibile all'indirizzo privacy@liquidlaw.it per qualsiasi richiesta di informazioni.

In qualità di Responsabile del Trattamento dei Dati, bSmart Labs s.r.l. assume il compito e la responsabilità di:

- adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, tra cui 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 le scuole 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 diverse prescrizioni di legge;
- mettere a disposizione 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 a bSmart Labs per l'esercizio di un diritto o reclamando una violazione, a comunicarlo alla scuola senza rispondere all'interessato, salvo diversa istruzione della scuola stessa;
- autorizzare il personale dedicato al trattamento dei dati, istruendolo adeguatamente e vincolandolo alla riservatezza;
- 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.

Registro delle attività di trattamento

bSmart Labs ha proceduto alla redazione del Registro delle Attività di Trattamento (nella versione "Titolare del Trattamento" e in quella da "Responsabile del Trattamento"). Considerata la centralità del Registro dei Trattamenti, si è deciso di rendere tale strumento realmente efficace per il controllo e la governance dei trattamenti, rendendolo quanto più completo possibile e al tempo stesso gestibile e dinamico (i contenuti definiti all'art. 30 del Reg. UE 2016/679 sono stati estesi in modo da fornire una visione del trattamento il più completa possibile).

Laddove necessario, bSmart Labs garantisce la possibilità di accedere al proprio registro delle attività di trattamento elaborato in qualità di Responsabile del Trattamento. La relativa richiesta può essere inoltrata a mezzo PEC all'indirizzo bsmart@legalmail.it.

Valutazione dei rischi per la sicurezza delle informazioni

bSmart Labs mantiene aggiornate le proprie valutazioni dei rischi per la sicurezza delle informazioni e per la protezione dei dati personali.

I DPO che volessero accedere alla metodologia ed ai dati riepilogativi delle valutazioni dei rischi o ricevere supporto per le DPIA possono rivolgersi al DPO di bSmart Labs.

Comunicazione di eventuali incidenti o potenziali violazioni

Qualunque incidente o potenziale incidente occorso tramite o durante l'utilizzo di un applicativo bSmart, che contempli o meno la presenza di dati personali, deve essere immediatamente comunicato agli appositi canali di assistenza bSmart (telefono, e-mail, o Ticket).

Il servizio assistenza bSmart prende in ogni caso in carico la segnalazione ed effettua una verifica preliminare sull'incidente, che comprende anche l'immediato indirizzamento di una tempestiva correzione, laddove applicabile e necessaria.

Nel caso in cui l'incidente, accertato, riguardasse anche dati personali, bSmart Labs effettua tutti i passaggi, sostanziali e formali, per la verifica della sussistenza, consistenza e modalità di gestione di un eventuale data breach, con la collaborazione e la supervisione del DPO.

In funzione del tipo e della gravità dell'incidente occorso ai dati personali, bSmart Labs documenta opportunamente il data breach nel "Registro delle violazioni dati personali" e procede alla comunicazione dello stesso al Titolare del Trattamento (nei casi in cui è stata nominata responsabile del trattamento).

In dipendenza del tipo e della gravità dell'incidente occorso, quindi, bSmart Labs può chiedere alla scuola segnalante la compilazione e trasmissione via PEC di apposita modulistica di segnalazione necessaria per la documentazione del data breach all'interno dei registri bSmart Labs e l'eventuale comunicazione ad altri soggetti (Titolari o Responsabili del Trattamento) coinvolti nell'incidente.